#2

500.40368X00

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE



Applicant(s): HONJO, et al

Serial No.: Not assigned

Filed: July 20, 2001

Title: ACCESS CONTROL METHOD

Group: Not assigned

LETTER CLAIMING RIGHT OF PRIORITY

Honorable Commissioner of
Patents and Trademarks
Washington, D.C. 20231

July 20, 2001

Sir:

Under the provisions of 35 USC 119 and 37 CFR 1.55, the applicant(s) hereby claim(s) the right of priority based on Japanese Patent Application No.(s) 2000-320645 filed October 20, 2000.

A certified copy of said Japanese Application is attached.

Respectfully submitted,

ANTONELLI, TERRY, STOUT & KRAUS, LLP

Carl I. Brundidge
Registration No. 29,621

CIB/amr
Attachment
(703) 312-6600

# 日本国特許庁
# JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２０００年１０月２０日

出願番号
Application Number: 特願２０００－３２０６４５

出願人
Applicant(s): 株式会社日立製作所

CERTIFIED COPY OF
PRIORITY DOCUMENT

２００１年 ６月 ６日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造

【書類名】　特許願
【整理番号】　K00018781
【あて先】　特許庁長官殿
【国際特許分類】　H04L　9/00
【発明者】
【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内
【氏名】　本城　信輔
【発明者】
【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内
【氏名】　洲崎　誠一
【特許出願人】
【識別番号】　000005108
【氏名又は名称】　株式会社日立製作所
【代理人】
【識別番号】　100077274
【弁理士】
【氏名又は名称】　磯村　雅俊
【電話番号】　03-3348-5035
【復代理人】
【識別番号】　100102587
【弁理士】
【氏名又は名称】　渡邉　昌幸
【電話番号】　03-3348-5035
【手数料の表示】
【予納台帳番号】　068262
【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9003100

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　個人情報の信頼度および開示度による認証またはアクセス管理システム、および管理方法

【特許請求の範囲】

【請求項１】　ネットワークに接続されたユーザ端末と、

該ユーザ端末からのチケット発行要求に応じて、個人情報データベースに登録された当該ユーザの個人情報を取出し、チケットを作成して該ユーザ端末に返送するチケット発行サーバと、

必要な情報、該情報の開示レベルおよび該情報の承認の要不要を内容とするサーバ・ポリシを設定し、アクセス条件が要チケットの場合には、各ユーザ端末に該サーバ・ポリシと要チケットを通知して、アクセス要求を受信した場合には、添付されたチケットの内容と該サーバ・ポリシを照合してアクセス可能か否かを判別するアクセス制御サーバと

を有することを特徴とする個人情報の信頼度および開示度による認証またはアクセス管理システム。

【請求項２】　請求項１に記載の個人情報の信頼度および開示度による認証またはアクセス管理システムにおいて、

前記チケットは、一つ以上の個人情報および該個人情報に関する属性情報を記載したデータと、該チケットの発行元の第三者機関によって該データに施されたデジタル署名とを内容とし、

アクセス制御サーバが示すポリシに従って開示情報を制御する証明書であり、該アクセス制御サーバにより検証されることを特徴とする個人情報の信頼度および開示度による認証またはアクセス管理システム。

【請求項３】　クライアントからのアクセス要求を受信すると、アクセス制御に要チケットか否か、該アクセス要求にチケットが添付してあるか否か、該チケットが正当なものであるか否か、当初設定したサーバ・ポリシと照合して一致するか否か、をそれぞれ判別することにより、アクセス制御を行うことを特徴とするアクセス制御サーバ装置。

【請求項４】　クライアントからのチケット要求を受信すると、該チケット要求に添付されたサーバ・ポリシおよびアクセス希望ディレクトリを解析し、希望ディレクトリにアクセスするために必要な個人情報、承認の必要性、および開示の必要性を調べ、データベースから必要な情報を取得してチケットを作成し、作成したチケットを上記クライアントに送信することを特徴とするチケット発行サーバ装置。

【請求項５】　アクセス制御サーバはサーバ・ポリシを設定し、クライアントからのアクセス要求を受けると、アクセスに要チケットか否かを確認して、要チケットの場合にはチケット要求と上記サーバ・ポリシを該クライアントに通知し、

該クライアントはチケット発行サーバに上記サーバ・ポリシを添付してチケット要求を送信し、

該チケット発行サーバは、該サーバ・ポリシを解析して必要な情報を用いてチケットを生成し、該クライアントに生成したチケットを送信し、

該クライアントは受信したチケットを保存するとともに、該チケットを添付してアクセス制御サーバにアクセス要求を送信し、

該アクセス制御サーバは、添付されたチケットを検証するとともに、該サーバ・ポリシと照合して検証することにより、アクセスを許可または不許可とすることを特徴とする個人情報の信頼度および開示度による認証またはアクセス管理方法。

【請求項６】　チケット発行サーバは、クライアントからのチケット要求を受信すると、セッション鍵を生成し、必要な情報および該セッション鍵を記載したチケットを発行し、該チケットをアクセス制御サーバの公開鍵で暗号化し、暗号化したチケットとセッション鍵を上記クライアントに送信し、

該クライアントは、受信したチケットとセッション鍵を保存するとともに、該セッション鍵でアクセス要求時刻を暗号化して認証子を作成し、アクセス制御サーバに対して該認証子と暗号化されたチケットとを添付してアクセス要求を送信し、

該アクセス制御サーバは、上記暗号化されたチケットを復号化して、該チケッ

トからセッション鍵を取り出し、該セッション鍵で該認証子を復号化し、得られた時刻を検証するとともに、該チケットおよびサーバ・ポリシを検証して、アクセスを許可するか否かを決定することを特徴とする個人情報の信頼度および開示度による認証またはアクセス管理方法。

【請求項７】　請求項５または６に記載の個人情報の信頼度および開示度による認証・アクセス管理方法の各処理ステップをプログラムに変換し、該プログラムを記録媒体に格納したことを特徴とするコンピュータにより読み出し可能なプログラム記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、信頼のある個人情報をもとに個人情報を秘匿してアクセス管理を行うことを可能にした個人情報の信頼度および開示度による認証またはアクセス管理システムおよび管理方法に関する。

【０００２】

【従来の技術】

従来、認証方法としてはユーザＩＤやパスワードを使用した認証方法、または公開鍵暗号系を使用する方法（例えば、ＳＳＬ（Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔ　Ｌａｙｅｒ）が用いられてきた。

ユーザＩＤやパスワードによる認証方法は、あらかじめ登録されたユーザＩＤやパスワードに合致することを検証する方法と、ユーザＩＤとパスワードから秘密鍵を生成して、これを保持していることを証明することによって検証する方法がある。

公開鍵暗号系では、暗号系と復号化に異なった鍵を用い、復号鍵を秘匿しておき、暗号鍵を公開する。

公開鍵暗号系における認証は、この暗号鍵を保持していることを何らかの形で証明することで行われる。

この公開された暗号鍵は、名前、組織名、有効期限などの情報とともに、公開鍵証明書に格納され、この公開鍵証明書を参照することにより認証する相手の身

元の情報を得ることができる。

【０００３】

【発明が解決しようとする課題】

しかしながら、従来の認証・アクセス方法では、下記のような問題点があった。１）ユーザの身元がわかってしまうこと、すなわち、認証技術であるから当然のことであるが、身元を明かして認証をもらう必要がある。しかし、匿名で投稿をしたいときや、身元を隠して掲示板に書き込みたいときなど、身元を隠してアクセスしたい場合があるが、従来の方法では認証が受けられないという問題があった。

２）ユーザ登録が必要であること、すなわち、予めアクセスを許可するユーザを決めておく必要がある。しかし、身元を確実にすることは必要であるが、アクセスする際だけは身元を隠しておきたい場合があるという問題がある。

３）ユーザのアクセス許可の設定が一元的であること、すなわち、認証側では、登録されたユーザＩＤだけを検証して、許可するか否かの判断材料になっていた。しかし、ユーザ側としては、他の情報も判断の材料にしたいという要望がある。

【０００４】

例えば、女性だけアクセスを許可する掲示板を設置したい場合があるが、このときには性別のみの認証を得ていればよいことになる。また、１８才以上の者しか見られない成人向けのサイトを設置する場合には、１８才以上という年令のみの認証を得ていればよいことになる。また、匿名の投稿をしたいときには、アクセスされる側としては、誹謗中傷など問題のあった場合に送信者が特定できる必要がある。また、匿名のハンドル名で何回か投稿されたときに、それらが本当に同じ送信者によるものであることを保証する方法があればよい訳である。

しかし、従来の認証技術では、性別のみの認証、年令のみの認証はできなかった。また、他人によるなりすましが可能になっていた。

【０００５】

そこで、本発明の目的は、これら従来の課題を解決し、信頼のある個人情報をもとにアクセス管理を行い、かつ個人情報を秘匿してアクセスが可能な個人情報

の信頼度および開示度による認証またはアクセス管理システム、および管理方法を提供することにある。

【０００６】

【課題を解決するための手段】

上記目的を達成するため、本発明の認証またはアクセス管理システムは、ネットワークに接続されたユーザ端末と、該ユーザ端末からのチケット発行要求に応じて、個人情報データベースに登録された当該ユーザの個人情報を取出し、チケットを作成して該ユーザ端末に返送するチケット発行サーバと、必要な情報、該情報の開示レベルおよび該情報の承認の要不要を内容とするサーバ・ポリシを設定し、アクセス条件が要チケットの場合には、各ユーザ端末に該サーバ・ポリシと要チケットを通知して、アクセス要求を受信した場合には、添付されたチケットの内容と該サーバ・ポリシを照合してアクセス可能か否かを判別するアクセス制御サーバとを有することを特徴としている。

上記チケットは、一つ以上の個人情報および該個人情報に関する属性情報を記載したデータと、発行元の第三者機関によって該データに施されたデジタル署名から構成されるもので、ポリシーに従って開示情報を制御した証明書とみなすことができる。

個人情報はサーバ・ポリシに従ってチケットに直接記載するか、または、直接記載しない場合は開示しない旨をチケットに記載する。

また、該個人情報に関する属性情報の例としては、個人情報の信頼度、すなわち該個人情報が第三者機関によって承認された情報であるか否かを示す情報が挙げられる。

個人情報の信頼度の設定の方法は、例えば、生年月日を登録時に確認する第三者機関は、生年月日を承認された情報としてチケットに設定できるが、登録時に生年月日の確認を行わない第三者機関は、生年月日を未承認な情報としてチケットに設定する。

【０００７】

【発明の実施の形態】

以下、本発明の原理および実施例を、図面により詳細に説明する。

（原理）

本発明の認証またはアクセス管理方法は、次の手順で行われる。

１）個人情報を第三者機関に登録する。これは、従来の認証技術と同じである。

２）アクセス制御を行うサーバに、その条件を記載したサーバ・ポリシを設定する。サーバ・ポリシの記載内容としては、対象ディレクトリ、必要な情報（例えば、名前や生年月日）、情報の開示レベル（名前を記載する必要があるか？）、情報の承認が必要か否か？例えば、ｈｔｔｐ：／／ｗｗｗ．ａｂｃ．ｃｏｍ／ｃｇｉ－ｂｉｎ／ａｂｃ（名前，開示不要，要承認）、（生年月日，要開示，要承認）

３）利用者は、第三者機関に必要な情報を承認してもらうために、チケットを発行してもらう。チケットの内容の例としては

（名前：非開示：承認、

生年月日：1969.9.17:承認

第三者機関：ＡＢＣ）

４）利用者は、チケットをサーバに提示、サーバは、チケットの内容とサーバ・ポリシとを照らし合わせ、アクセス可能か否かを判断する。

上記の例の場合には、第三者機関ＡＢＣによって、名前が承認されており、生年月日が開示され、かつ承認されているので、アクセスを許可する。

５）特に、匿名アクセス許可の後、問題が発生すれば、被害者または裁判所などの調停者はサーバ上の掲示板に、送信者に不適正な書き込みがあることを伝えることにより、サーバはチケット記載の情報を第三者機関に問い合わせ、第三者機関は送信者を特定し、特定した者に警告など所定の対処を施し、調停者などに対所を施したこと伝えるか、あるいは送信者の情報を提供する。

【０００８】

図１は、本発明の原理（解決手段１）を示す説明図であって、承認されたハンドル名によるアクセス制御の場合を示す。

図１において、１０は信頼できる第三者機関ＡＢＣであって、個人情報データベース１１を備えている。１１Ａは、個人情報データベースに登録された内容である。２０はユーザ（ここではｈｏｎｊｏ）、１２は第三者機関ＡＢＣ１０によ

り発行されたチケット内容、３０はアクセスを制御するサーバであって、３１はサーバ・ポリシの内容、３１Ａはサーバ・ポリシの送信内容である。

以下、①～⑦の手続きの番号に従って処理手順を説明する。先ず、①ユーザ２０は、第３者機関ＡＢＣ１２に対して個人情報の登録を行う。ここには、例えば、ユーザＩＤ、氏名、生年月日、住所、性別、ハンドル名が登録されている。次に、②ユーザ２０は、サーバ３０に対して掲示板Ａに書き込み希望を送信する。

アクセス制御サーバ３０は、サーバ・ポリシ３１として、掲示板Ａ：認証されたハンドル名でアクセスすること、化粧品ページＢ：アクセスできるのは女性であること、成人向けページＣ：アクセスできるのは１８才以上であること、を持っている。③サーバ３０は、ユーザ２０からの掲示板Ａへの書き込み希望に対して、サーバ・ポリシの内容３１Ａとチケットが必要である旨を返送する。

④ユーザ２０は、第三者機関ＡＢＣ１０に対してチケット発行希望（認証されたハンドル名を記載）する。⑤第３者機関ＡＢＣ１０は、チケット発行希望があると、個人情報データベース１１の内容を参照して、チケット１２をユーザに送信する。チケット１２の内容は、チケットＩＤと、ハンドル名（Ｊｂｏｙ）が第３者機関ＡＢＣにより承認されていることを記載して、改ざん防止のためにＡＢＣによるデジタル署名を行う。

⑥ユーザは、アクセス制御サーバ３０に対して、発行されたチケット１２を添付して、掲示板Ａへの書き込み希望を送信する。⑦アクセス制御サーバ３０は、チケット１２を検証し、アクセスの確認を行い、メッセージを返送する。

【０００９】

図２は、同じく原理（解決手段１）の承認されたハンドル名によるアクセス制御において、不適正な書き込みをした場合の手続を示す図である。

図１の手続において、ハンドル名Ｊｂｏｙが不適正な書き込み、例えば他人の中傷誹謗を書き込んだ場合、重大な不法行為をする決意を書き込んだ場合等には、被害者または裁判所などの調停者７０は、①サーバ上の掲示板に、Ｊｂｏｙによる不適正な書き込みがあることをサーバ３０に伝える。②アクセス制御サーバ３０は、該当する書き込みを特定し、対応するチケットＩＤを特定する。③サーバ３０は、第三者機関ＡＢＣ１０に対して、Ｊｂｏｙが不適正な書き込みをした

ことを伝える。チケットＩＤを送信する。④第三者機関ＡＢＣ１０は、個人情報データベース１１を検索して、Ｊｂｏｙは、ユーザｈｏｎｊｏであることが分かる。⑤第三者機関ＡＢＣ１０は、ユーザ２０に対して警告を与える。⑥第三者機関１０は、送信者を特定した後、被害者または調停者７０に対して、送信者にしかるべき対処を施したことを伝える。状況によっては、調停者７０に送信者の情報を提供することもある。

この結果、インターネットにおいて、個人情報を秘匿しても、本発明では身元保証が可能であるため、無責任な行動や犯罪が少なくなる。

【００１０】

図３は、本発明の原理（解決手段２）を示す説明図であって、性別によるアクセス管理を示す。

①ユーザ２０は、サーバ３０に対して化粧品ページＢに書き込み希望を送信する。②サーバ２０は、化粧品ページＢは女性だけがアクセスできる、というサーバ・ポリシ３１があること、要チケットであること、をユーザ２０に送信する。③ユーザ２０は、第三者機関ＡＢＣ１０に対してチケット発行希望（性別の証明）を送信する。④第三者機関ＡＢＣ１０はチケット発行希望があると、個人情報データベース１１の内容を参照して、チケット１２を発行し、ユーザ２０に送信する。チケット１２には、チケットＩＤと、このユーザは女性であることを記載し、ＡＢＣによるデジタル署名を行う。⑤ユーザ２０は、サーバ３０に対しチケット１２を添付して化粧品ページＢへの書き込み希望を送信する。⑥サーバ３０は、チケットを検証し、女性であるので、このアクセスを許可し、⑦ユーザ２０に対して化粧品ページＢを送信する。なお、不許可の場合には、化粧品ページＢを送信せずに、エラーメッセージを送信する。

【００１１】

（実施例１）

（ネットワーク構成）

図４は、本発明の実施例１を示すネットワークの構成図である。

図４において、４０は会社や大学等の私有の閉じられたネットワーク（いわゆるイントラネット）であり、５０はインターネット、３０はインターネット５０

に接続されたWWWサーバである。１０はチケット発行サーバであって、個人情報データベース１１を備えている。この場合、個人情報を把握している会社の人事課などがチケット発行サーバ１０になれば、都合がよい。２０はクライアントであって、WWWブラウザ２２に新たにチケット処理プラグインプログラム２１が追加されている。WWWサーバ３０には、サーバ・ポリシ３１が備えられるとともに、新たにチケット認証・アクセス管理部３２が設けられる。従来のブラウザ２２は、チケットを使えないため、チケットを使えるようにチケット認証・アクセス管理部３２を設けるとともに、チケット処理プラグインプログラム２１をブラウザ３２に付加される。

なお、将来、市町村の役所や個人情報を把握した団体などがチケット発行サーバ１０になる場合には、閉じたネットワーク４０に設置することなく、インターネット５０に直接設置することができる。

【００１２】

（クライアント構成）

図５は、図４におけるクライアントの詳細構成図である。

クライアント（端末）は、通信ケーブルを介してインターネットに接続されており、ネットワークインタフェース２８を経由してメインバスに接続される。メインバスには、端末全体を制御するＣＰＵ２４、プログラムなどを格納するメインメモリ、外部メモリであるハードディスク２５、インターネットの各情報などを表示する表示装置２６、マウスなどの入力装置２７が接続されている。メインメモリには、オペレーティングシステム２３、WWWブラウザプログラム２２およびチケット処理プラグインプログラム２１が格納される。チケット処理プラグインプログラム２１を実行することにより、第三者機関１０へのチケット発行要求や個人情報の登録などを自動的に行うことができる。

【００１３】

（チケット発行サーバ構成）

図６は、図４におけるチケット発行サーバの詳細構成図である。

チケット発行サーバ１０は、通信ケーブルを介してインターネットに接続されており、ネットワークインタフェース１７を経由してメインバスに接続される。

メインバスには、サーバ全体を制御するＣＰＵ１４、プログラムなどを格納するメインメモリ、外部メモリであるハードディスク１１、表示装置１５、入力装置１６が接続されている。メインメモリには、オペレーティングシステム１２とチケット発行プログラム１３が格納されている。チケット発行プログラム１３を実行することにより、通信ケーブルを介してチケット発行要求が送られてきたときには、自動的に一つ以上の押人情報とその個人情報に関する属性情報を記載し、発行元の第三者機関のデジタル署名を記載することができる。

【００１４】

（WWWサーバ構成）

図７は、図４におけるWWWサーバの詳細構成図である。

WWWサーバ（アクセス制御サーバ）３０は、通信ケーブルを介してインターネットに接続されており、ネットワークインタフェース３９を経由してメインバスに接続される。

メインバスには、サーバ全体を制御するＣＰＵ３５、プログラムなどを格納するメインメモリ、外部メモリであるハードディスク３６、表示装置３７、入力装置３８が接続されている。メインメモリには、オペレーティングシステム３４と、WWWサーバプログラム３３と、チケット認証・アクセス管理プログラム３２とが格納されている。このチケット認証・アクセス管理プログラム３２を実行することにより、通信ケーブルを介して掲示板などに書き込みするためのアクセス要求が送られてきたときに、自動的にチケットの認証およびアクセス管理を行うことができる。

【００１５】

（個人情報データベース）

図８は、本発明の実施例１を示す個人情報データベースのデータ構成図である。

図８に示すように、個人情報データベースには、ユーザＩＤ、氏名、連絡先（住所）、生年月日、性別、ハンドル名、所属、メールアドレス、が記載されている。

【００１６】

（サーバ・ポリシ）

図９は、本発明の実施例１を示すサーバ・ポリシの内容例を示す図である。

サーバ：ｗｗｗ．ａｂｃ．ｃｏｍ．のサーバ・ポリシとして、３つの例が記載されている。

１）サービス：掲示板

必要な情報：ハンドル名、要承認、開示

必要な情報：氏名、要承認、非開示

必要な情報：連絡先、要承認、非開示

（この掲示板には、承認が必要であり、かつ開示が必要なハンドル名と、開示する必要はないが、承認が必要な氏名と、開示する必要はないが、承認が必要な連絡先とが必要な情報となっている。）

２）サービス：女性専用ページ

必要な情報：ハンドル名、要承認、開示

必要な情報：性別＝‘女’，要承認、開示

（このページには、承認が必要であり、かつ開示が必要なハンドル名と、承認が必要で、かつ開示も必要な‘女’である性別情報が必要な情報となっている）

３）サービス：映画情報ページ（暴力シーン・性的なシーンあり）

必要な情報：年令≧‘１８’，要承認、開示

（このページには、承認が必要であり、かつ開示が必要な‘１８才’という年令が必要な情報となっている）

また、サーバ・ポリシは、マークアップ言語であるＸＭＬで記述され、従ってソフトウェアで柔軟に処理することが可能である。

【００１７】

（チケット）

図１０は、本発明の実施例１を示すチケットのデータ構成図である。

チケットは、マークアップ言語であるＸＭＬで記述され、従ってソフトウェアで柔軟に処理することが可能である。チケットは、一つ以上の個人情報とその個人情報に関する属性情報を記述したデータと、発行元の第三者機関によってこれらのデータに施されたデジタル署名から構成される。そして、ＷＷＷサーバ３０

が示すポリシに従って開示情報を制御した証明書とみなすことができる。

図１０に示すチケットには、チケットＩＤ、ハンドル名（承認されているか否か）、生年月日（承認されているか否か）、性別（承認されているか否か）、所属（承認されているか否か）、有効期間（年月日時）、チケット発行者、チケット発行者連絡先、およびデジタル署名が記載されている。

【００１８】

（１回目のやりとり）

図１１は、本発明の実施例１を示す１回目のやりとりのシーケンスチャートである。

図１１は、図１で前述した方法と同じ手順でやりとりが行われる。先ず、クライアントからWWWサーバに対してアクセス要求を行うと、WWWサーバはアクセス確認を行い、チケットが必要であるか否かを判断し（ステップ３００）、クライアントに対してチケット要求とサーバ・ポリシを返信する。クライアントは、チケット発行サーバに対してチケット要求を行い、サーバ・ポリシを付加して送信する。チケットサーバは、チケットを生成して（ステップ１００）、クライアントにそのチケットを送信する。クライアントは、受取ったチケットを保存し（ステップ２００）、WWWサーバに対してチケットを付加してアクセス要求を送信する。WWWサーバは、チケットを検証し、認証・アクセス制御を行い（ステップ３０１）、許可するときには、クライアントに対してＨＴＭＬページを送信する。不許可のときには、エラーを送信する。

【００１９】

（２回目以降のやりとり）

図１２は、本発明の実施例１を示す２回目のやりとりのシーケンスチャートである。

図１２では、チケットを発行してもらい、チケットを保存しているクライアントの動作を示している。クライアントは、WWWサーバに対して保存しているチケットを付加してアクセス要求を送信する。WWWサーバは、チケットの検証と認証・アクセス制御を行い（ステップ３０１）、許可のときには、ＨＴＭＬページをクライアントに返信する。なお、チケットの有効期限が切れたときには、再

度、チケット発行サーバに対してチケットの発行要求を送信する。

【００２０】

（クライアント処理）

図１３は、本発明の実施例１を示すクライアントの処理フローチャートである。

図１３における縦線の左側は従来技術のＷＷＷブラウザの処理であり、右側は本発明で新たに備えられるチケット処理プラグインプログラムの処理である。

ＷＷＷブラウザによりＷＷＷサーバへアクセス要求を行うと、アクセス対象の有効なサーバ・ポリシを持っているか否かを判断し（ステップ２０１）、持っている場合には、アクセス対象に利用可能な有効なチケットを持っているか否かを判断し（ステップ２０２）、持っている場合には、そのチケットを添付して、ＷＷＷサーバへアクセス要求を行う（ステップ２０３）。ＷＷＷサーバから『アクセス不可』のメッセージを受信しなければ（ステップ２０８）、該当するページを受信して（ステップ２０９）、ＷＷＷブラウザに渡し、ブラウザが画面に該当ページを表示する。

一方、アクセス対象の有効なサーバ・ポリシを持っていない場合には（ステップ２０１）、ＷＷＷサーバへアクセス要求を行い（ステップ２０４）、ＷＷＷサーバから要チケットメッセージとサーバ・ポリシを受信する（ステップ２０５）。また、アクセス対象に利用可能な有効なチケットを持っていない場合には（ステップ２０２）、チケット発行サーバに対してチケット発行要求を行い、サーバ・ポリシおよびアクセス希望ディレクトリを添付して送信する（ステップ２０６）。チケット発行サーバからチケットを受信すると、後の利用のためにこれを保存する（ステップ２０７）。そして、このチケットを添付してＷＷＷサーバにアクセス要求を行う（ステップ２０３）。また、ＷＷＷサーバから、『アクセス不可』のメッセージを受信した場合には（ステップ２０８）、エラー処理を行う（ステップ２１０）。

【００２１】

（ＷＷＷサーバの処理）

図１４は、本発明の実施例１を示すＷＷＷサーバの処理フローチャートである

。

ＷＷＷクライアントからアクセス要求を受信すると、アクセス制御確認を行い、チケットが必要か否かを判断し（ステップ３０１）、チケットが必要な場合には、チケットが要求に添付してあるか否かを判断する（ステップ３０２）。添付してあれば、それが正当なチケットであるか否かを判断する（ステップ３０３）。正当なチケットであれば、アクセスＯＫであるか否かを判断、すなわちサーバ・ポリシに合致するか否かを判断し（ステップ３０４）、ＯＫであれば、当該するページをクライアントに送信する（ステップ３０５）。

一方、アクセス制御確認で、チケットが必要でなければ（ステップ３０１）、当該するページをクライアントに送信する（ステップ３０６）。また、チケットが要求に添付していない場合には（ステップ３０２）、『要チケット』メッセージをクライアントに送信する（ステップ３０７）。また、正当なチケットでないか、あるいはアクセスＯＫでない場合には（ステップ３０３，３０４）、『アクセス不可』のメッセージをクライアントに送信する（ステップ３０８）。

【００２２】

（チケット発行サーバの処理）

図１５は、本発明の実施例１を示すチケット発行サーバの処理フローチャートである。

ＷＷＷクライアントからのチケット発行要求を受信すると、チケット発行サーバは、サーバ・ポリシ、アクセス希望ディレクトリを受信し（ステップ１０１）、サーバ・ポリシを解析して、希望ディレクトリにアクセスするために必要な個人情報、承認の必要性、開示の必要性を調べる（ステップ１０２）。個人情報データベースにアクセスし、必要な情報を取得する（ステップ１０３）。取得した情報に基づいてチケットを作成する（ステップ１００）。そのチケットをクライアントに送信する。

【００２３】

（実施例２）

（チケット）

図１６は、本発明の実施例２を示すチケットのデータ構成図である。

実施例２の特徴は、①チケットの内容全体がＷＷＷサーバの公開鍵で暗号化されていること、②チケットには、ＷＷＷサーバとクライアントで共有するセッション鍵が記載されていること、③チケット発行サーバはクライアントにセッション鍵を送信すること、④クライアントは受信したセッション鍵で認証子を作成すること、⑤ＷＷＷサーバに対して暗号化チケットと認証子を添付してアクセスを要求すること、⑥ＷＷＷサーバは、チケットからセッション鍵を取り出し、その鍵で認証子を復号化し、確かに本人から要求されたか否かを検証すること、を有しており、実施例１よりもさらに厳しい検証を受けてアクセスが許可されることになる。

図１６に示すように、チケットの内容は実施例１の場合と同じ内容に、セッション鍵が追加されている。すなわち、ＷＷＷサーバとクライアントで共有するセッション鍵を、チケット発行サーバが生成して、利用するＷＷＷサーバの公開鍵でチケットの内容を暗号化する。従って、クライアントには、暗号化されたチケットが送信される。

【００２４】

（認証子）

図１７は、本発明の実施例２を示す認証子の作成および検証の方法の説明図である。

実施例２では、認証子が必要となるが、これはチケットの正当な保持者であることを証明するためのものである。

実施例２では、実施例１の手続きに、チケットの不正利用防止機構を追加した手続きを採用する。チケット不正利用防止機構は、公知のＫｅｒｂｅｒｏｓの技術を利用する。すなわち、実施例１の方法を採用した場合、悪意を持った者がクライアントのやりとりを監視して、後で同一データをＷＷＷサーバに送信すれば、正当なクライアントになりすましてアクセスが可能になってしまうおそれがある。これを防止するために、Ｋｅｒｂｅｒｏｓの技術では、一般にアクセスを要求する時刻をセッション鍵で暗号化する方法を採用している。

【００２５】

図１７に示すように、認証子の作成は、要求時刻（例えば、2000年9月1日13:1

3)６０をセッション鍵で暗号化して、認証子を作成する。

次に、WWWサーバによる認証子の検証は、送信された認証子を同じセッション鍵で復号化する。これにより、要求時刻：(2000年9月1日13:13)６２が得られる。WWWサーバは、要求時刻が現在の時刻から許容範囲内にあるか否か、および、許容範囲内の場合、その範囲内に同じ時刻の認証子を受信していないかを確認することにより、不正に他人が同じ認証子を再送することを防止することができる。もし、正当なクライアントが送信した認証子を利用して、不正にアクセスする者がWWWサーバにアクセス要求をしても、その認証子は以前に正当なクライアントがアクセスした時刻であるため、許容範囲より外れている場合は、検証の結果、不正アクセスと判断される。

また、WWWサーバは、許容時刻の範囲だけ過去の認証子を記憶しておけばよい。

認証子を作成したり、検証できる者は、セッション鍵を知っている者、つまり正当なクライアントとWWWサーバであり、それ以外の者は認証子を作成したり、検証したりすることは不可能である。

【００２６】

（１回目のやりとり）

図１８は、本発明の実施例２を示す１回目のやりとりのシーケンスチャートである。

クライアントはWWWサーバに対してアクセス要求を行うと、WWWサーバはアクセスを確認し、要チケットであるか否かを判断する（ステップ３００Ａ）。WWWサーバはクライアントにチケット要求とサーバ・ポリシを添付して返送する。クライアントはチケット発行サーバに対して、チケット要求およびサーバ・ポリシを送信する。ここまでは、実施例１と同じである。チケット発行サーバは、セッション鍵を生成するとともに、チケットを生成する（ステップ１００Ａ）。チケット発行サーバは、生成したチケットとセッション鍵をクライアントに送信する。クライアントは、セッション鍵とチケットを保存し、セッション鍵で認証子を作成する（ステップ２００Ａ）。そして、WWWサーバに対して、チケットと認証子を添付してアクセス要求を行う。WWWサーバは、認証子とチケット

検証を行うとともに、認証・アクセス制御を行う（ステップ３０１Ａ）。検証の結果、許可するときには、クライアントにＨＴＭＬページを送信する。

【００２７】

（クライアントの処理）

図１９は、本発明の実施例２を示すクライアントの処理フローチャートである。

ＷＷＷブラウザにより、ＷＷＷサーバへアクセス要求を行うことで、アクセス対象の有効なサーバ・ポリシを持っているか否かを判断し（ステップ２０１）、持っている場合には、アクセス対象に利用可能な有効なチケットを持っているか否かを判断する（ステップ２０２）。両方とも持っている場合には、時刻をセッション鍵で暗号化して認証子を作成する（ステップ２０２Ａ）。そして、チケットと認証子を添付してＷＷＷサーバにアクセス要求を行う（ステップ２０３Ａ）。ＷＷＷサーバから『アクセス不可』のメッセージを受信しない場合には（ステップ２０８）、当該するページを受信する（ステップ２０９）。このページをＷＷＷブラウザに渡すことにより、ブラウザは画面にこのページを表示する。

一方、アクセス対象の有効なサーバ・ポリシを持っていない場合には（ステップ２０１）、ＷＷＷサーバにアクセス要求を行い（ステップ２０４）、ＷＷＷサーバから要チケットメッセージとサーバ・ポリシを受信する（ステップ２０５）。また、アクセス対象に利用可能な有効なチケットを持っていない場合には（ステップ２０２）、チケット発行要求を行い、サーバ・ポリシおよびアクセス希望ディレクトリをチケット発行サーバに送信する（ステップ２０６）。チケット発行サーバからチケット、セッション鍵を受信して、後の利用のためにこれらを保存する（ステップ２０７Ａ）。そして、時刻をセッション鍵で暗号化して認証子を作成し（ステップ２０２Ａ）、チケットと認証子を添付してＷＷＷサーバにアクセス要求を行う（ステップ２０３Ａ）。『アクセス不可』のメッセージを受信した場合には（ステップ２０８）、エラー処理を行う（ステップ２１０）。

【００２８】

（ＷＷＷサーバの処理）

図２０は、本発明の実施例２を示すＷＷＷサーバの処理フローチャートである

。

ＷＷＷクライアントからのアクセス要求を受信すると、アクセス制御確認を行い、要チケットであるか否かを判断する（ステップ３０１）。要チケットであれば、チケット、認証子が要求に添付してあるか否かを判断する（ステップ３０２）。添付してあれば、正当なチケットであるか否かを判断する（ステップ３０３）。正当なチケットであれば、認証子の検証はＯＫか否かを判断する（ステップ３０３１）。検証が許可範囲内にあれば、アクセスＯＫか否かを判断、すなわちサーバ・ポリシに合致するか否かを判断し（ステップ３０４）、ＯＫであれば、該当するページをクライアントに送信する（ステップ３０５）。

一方、要チケットでない場合には（ステップ３０１）、該当するページをクライアントに送信する（ステップ３０６）。また、チケット、認証子が要求に添付していない場合には（ステップ３０２Ａ）、『要チケット』メッセージをクライアントに送信する（ステップ３０７）。また、正当なチケットでないか、あるいは認証子の検証がＮＯであるか、あるいはアクセスＯＫでないか（サーバ・ポリシに不一致）のいずれかであれば（ステップ３０３，３０３１，３０４）、『アクセス不可』のメッセージをクライアントに送信する（ステップ３０８）。

【００２９】

（チケット発行サーバの処理）

図２１は、本発明の実施例２を示すチケット発行サーバの処理フローチャートである。

ＷＷＷクライアントからのチケット発行要求を受信すると、チケット発行サーバは、チケット発行要求に添付されているサーバ・ポリシ、アクセス希望ディレクトリを受信する（ステップ１０１）。次に、サーバは、サーバ・ポリシを解析し、希望ディレクトリにアクセスするために必要な個人の情報、承認の必要性、開示の必要性を調べる（ステップ１０２）。次に、個人情報データベースにアクセスして、必要な情報を取得し（ステップ１０３）、セッション鍵を作成し（ステップ１０４）、チケットを作成する（ステップ１００）。作成したチケットと、セッション鍵をクライアントに送信する。

【００３０】

〈実施例２の詳細フロー〉

図２２は、本発明の実施例２を示す認証またはアクセス管理方法の詳細フローチャートである。

チケット発行サーバは、クライアントからチケット発行要求を受けると、セッション鍵を生成し、チケットを発行して、生成したセッション鍵を記載した後、そのチケットをWWWサーバの公開鍵で暗号化する（ステップ１００Ｂ）。そして、クライアントに対して、暗号化したチケットと生成されたセッション鍵を送信する。

クライアントは、受信したチケットおよびセッション鍵を保存し、現在の時刻をセッション鍵で暗号化して認証子を作成する（ステップ２００Ｂ）。そして、WWWサーバに対して、暗号化したチケットおよび作成した認証子を添付してアクセス要求を行う。

WWWサーバは、暗号化したチケットを復号化する。そして、セッション鍵を取り出す。このセッション鍵で認証子を復号化して時刻を取り出す。次にその時刻を検証する。受信時刻の許容範囲内にあれば、確かにクライアント本人であることを判別する。また、チケット・サーバ・ポリシを検証し、合致していれば、アクセスＯＫと判断する。

アクセスＯＫの場合には、クライアントに対してＨＴＭＬページを送信する。

もし、アクセスＮＯの場合には、アクセス不可を送信することにより、クライアントはエラー処理を行う。

【００３１】

（プログラム記録媒体）

図１３（実施例１のWWWブラウザの処理）、図１４（同WWWサーバの処理）、図１５（同チケット発行サーバの処理）、図１９（実施例２のクライアントの処理）、図２０（同WWWサーバの処理）、図２１（同チケット発行サーバの処理）、および図２２（同実施例２の処理手順）の各処理ステップをプログラムに変換し、そのプログラムをＣＤ－ＲＯＭなどの記録媒体に格納しておく。これにより、インターネットに接続された任意の端末のパソコンに実装し、プログラムをインストールするか、あるいはネットワークを介して他のパソコンにダウン

ロードして、プログラムを実施すれば、本発明を容易に実現することができる。

【００３２】

【発明の効果】

以上説明したように、本発明によれば、信頼のある個人情報を基にアクセス管理が可能になるとともに、個人情報を秘匿しながらの身元保証が可能となる。これにより、匿名の投稿が可能になり、信頼できるハンドル名の使用が可能となる。また、女性だけのアクセス許可や、年令制限を有するアクセス許可が可能となる。

【図面の簡単な説明】

【図１】

本発明の原理（アクセス制御の解決手段１）を示す説明図である。

【図２】

本発明の原理（不適正書込みの解決手段１）を示す説明図である。

【図３】

本発明の原理（性別によるアクセス管理の解決手段２）を示す説明図である。

【図４】

本発明の実施例１を示すネットワークの構成図である。

【図５】

図４におけるクライアントの詳細構成図である。

【図６】

図４におけるチケット発行サーバの詳細構成図である。

【図７】

図４におけるＷＷＷサーバの詳細構成図である。

【図８】

本発明の実施例１を示す個人情報データベースのデータ構成図である。

【図９】

本発明の実施例１を示すサーバ・ポリシのデータ構成図である。

【図１０】

本発明の実施例１を示すチケットのデータ構成図である。

【図１１】

本発明の実施例１を示す１回目のやりとりのシーケンスチャートである。

【図１２】

同２回目以降のやりとりのシーケンスチャートである。

【図１３】

本発明の実施例１を示すクライアントの処理フローチャートである。

【図１４】

本発明の実施例１を示すＷＷＷサーバの処理フローチャートである。

【図１５】

本発明の実施例１を示すチケット発行サーバの処理フローチャートである。

【図１６】

本発明の実施例２を示すチケットのデータ構成図である。

【図１７】

本発明の実施例２を示す認証子の作成および検証の説明図である。

【図１８】

本発明の実施例２を示す１回目のやりとりのシーケンスチャートである。

【図１９】

本発明の実施例２を示すクライアントの処理フローチャートである。

【図２０】

本発明の実施例２を示すＷＷＷサーバの処理フローチャートである。

【図２１】

本発明の実施例２を示すチケット発行サーバの処理フローチャートである。

【図２２】

本発明の実施例２を示す詳細処理のフローチャートである。

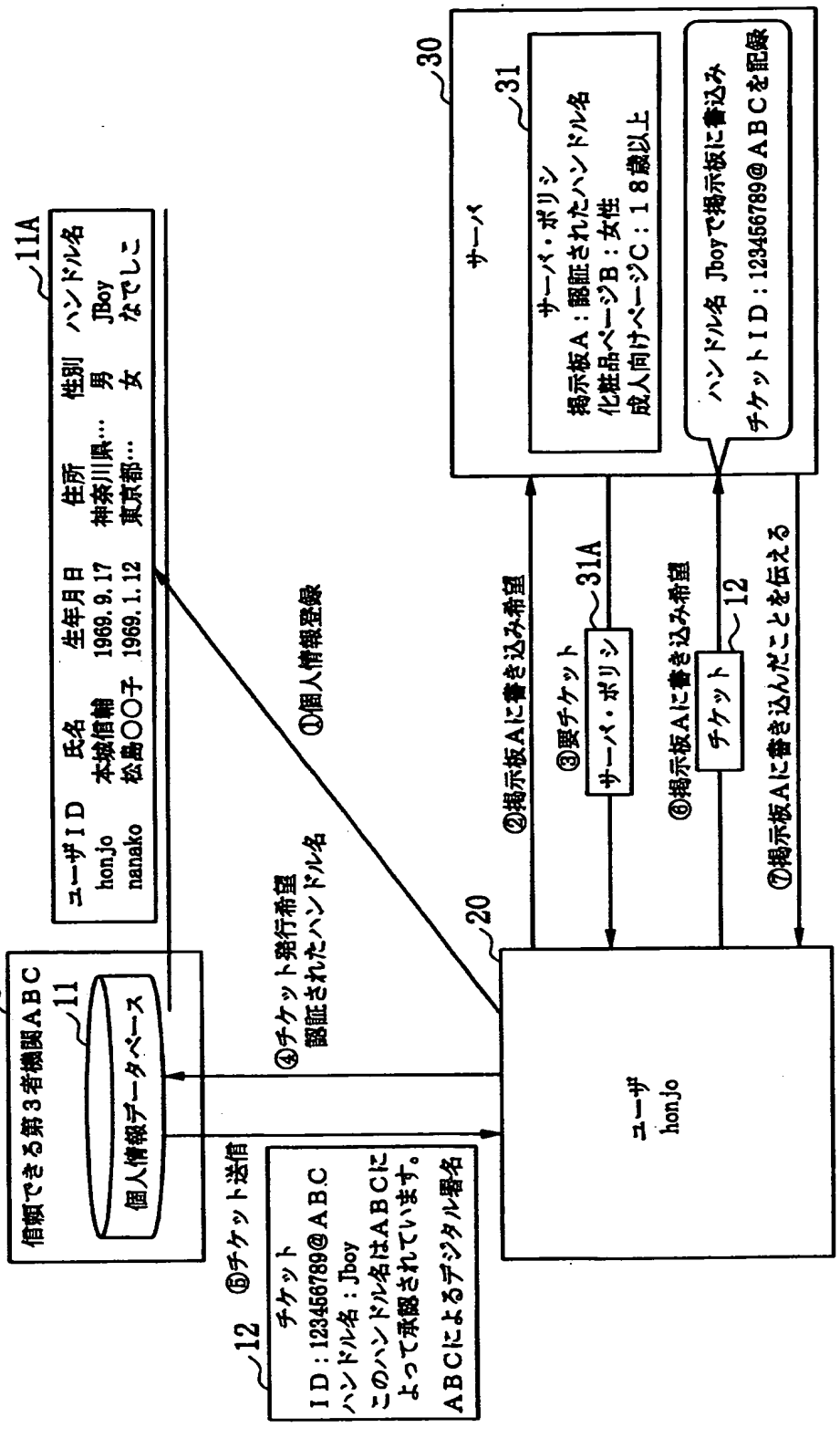
【符号の説明】

１０…信頼できる第三者機関ＡＢＣ、２０…ユーザ、３０…ＷＷＷサーバ、
１１…個人情報データベース、１２…チケット、３１…サーバ・ポリシ、
４０…ネットワーク、５０…インターネット、１４，２４，３５…ＣＰＵ、
１３…チケット発行プログラム、２５，３６…ハードディスク、

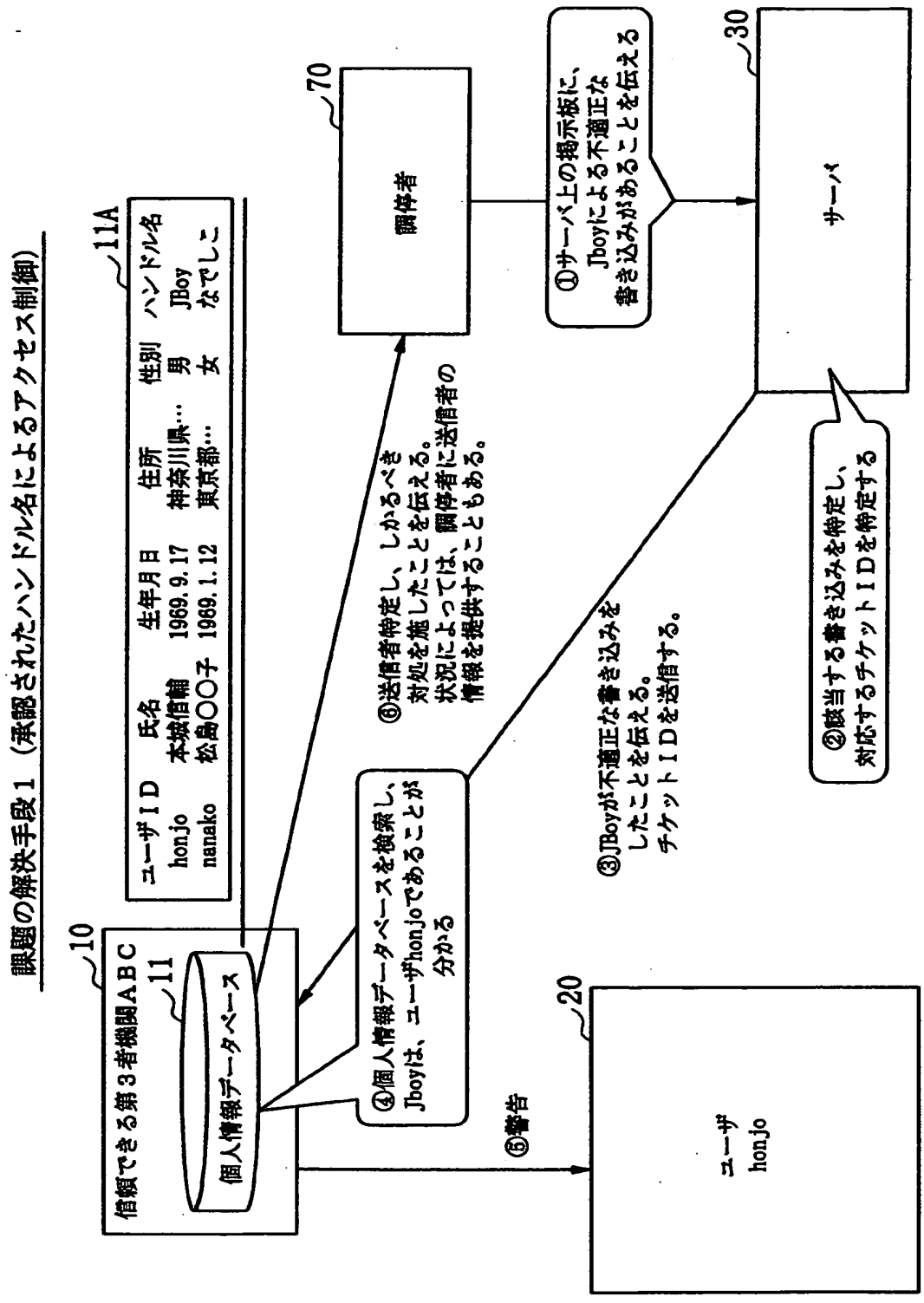
１２，２３，３４…オペレーティングシステム、
１５，２６，３７…表示装置、１６，２７，３８…入力装置、
１７，２８，３９…ネットワークインターフェース、
２２…WWWブラウザプログラム、３３…WWWサーバプログラム、
２１…チケット処理プラグインプログラム、７０…調停者、
３２…チケット認証・アクセス管理プログラム、６０…要求時刻、
６１…認証子、６２…復号化された時刻。

【書類名】　図面

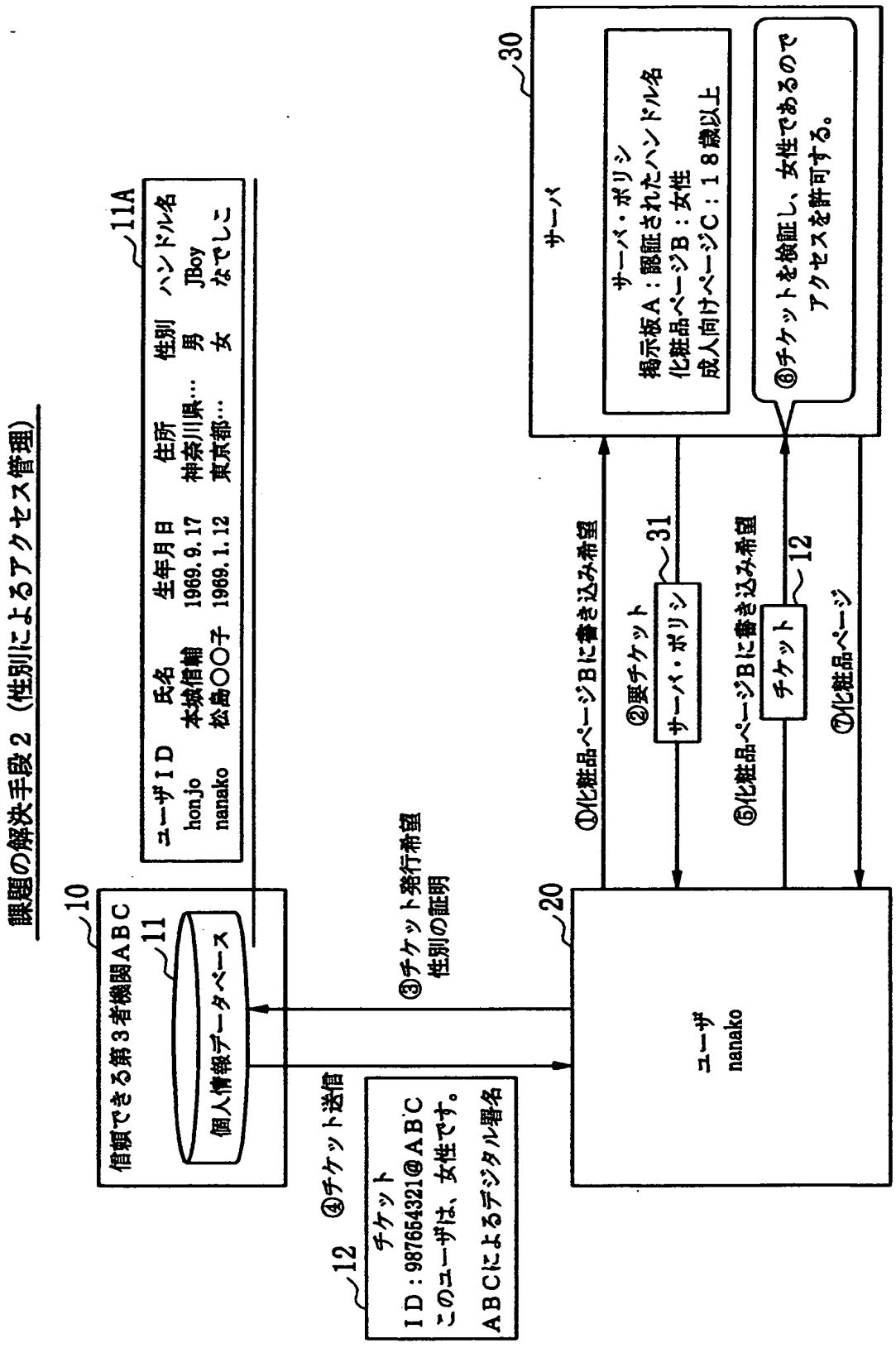
【図１】


課題の解決手段１（承認されたハンドル名によるアクセス制御）
信頼できる第３者機関ＡＢＣ
10
11
個人情報データベース
11A
ユーザＩＤ　氏名　生年月日　住所　性別　ハンドル名
honjo　本城信輔　1969.9.17　神奈川県…　男　JBoy
nanako　松島○○子　1969.1.12　東京都…　女　なでしこ
⑤チケット送信
12
チケット
ＩＤ：123456789@ＡＢＣ
ハンドル名：Jboy
このハンドル名はＡＢＣによって承認されています。
ＡＢＣによるデジタル署名
④チケット発行希望
認証されたハンドル名
①個人情報登録
20
ユーザ
honjo
②掲示板Ａに書き込み希望
③要チケット
31A
サーバ・ポリシ
⑥掲示板Ａに書き込み希望
チケット
12
⑦掲示板Ａに書き込んだことを伝える
30
サーバ
31
サーバ・ポリシ
掲示板Ａ：認証されたハンドル名
化粧品ページＢ：女性
成人向けページＣ：１８歳以上
ハンドル名 Jboyで掲示板に書込み
チケットＩＤ：123456789@ＡＢＣを記録

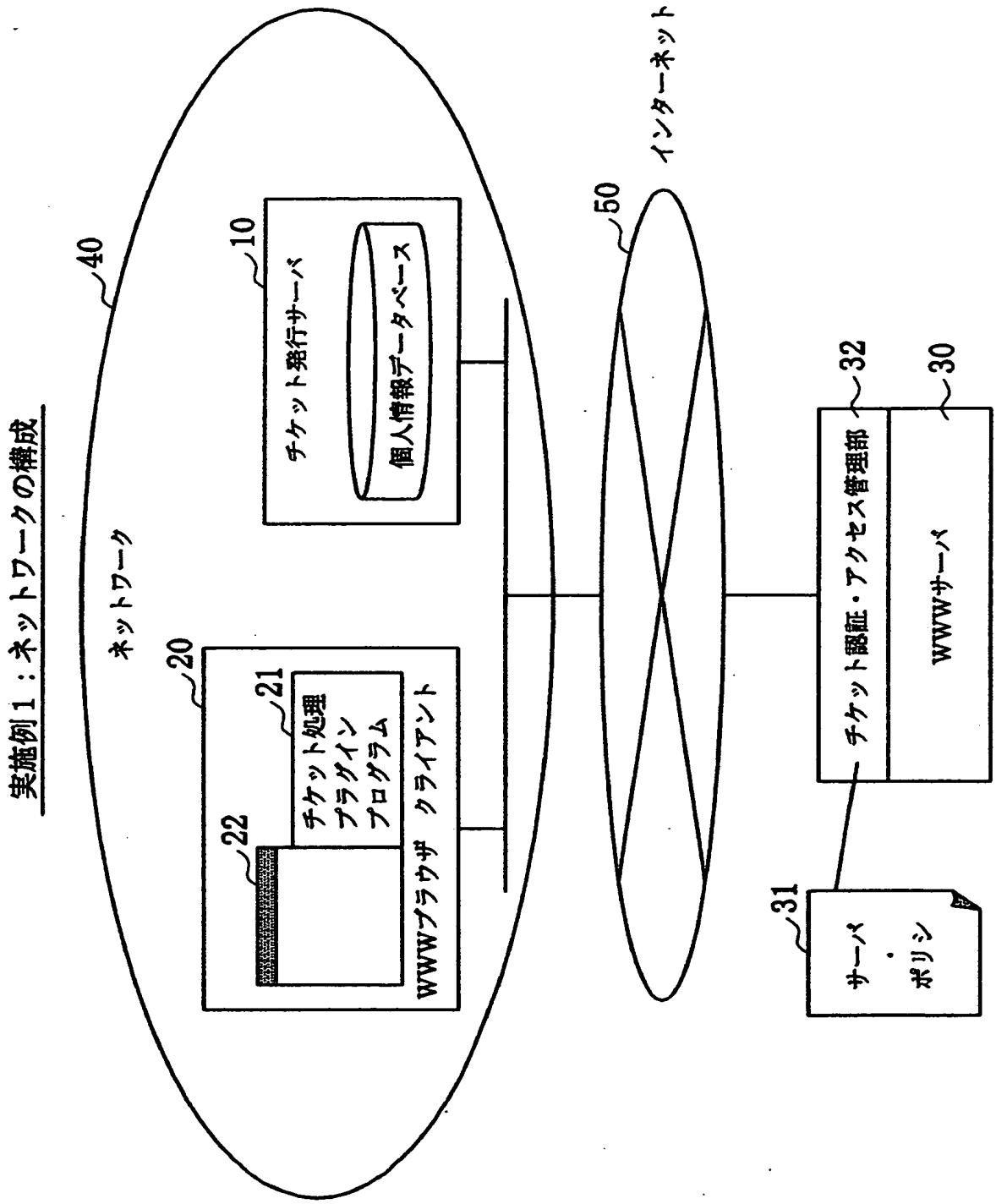
【図２】


課題の解決手段１（承認されたハンドル名によるアクセス制御）
信頼できる第３者機関ＡＢＣ
10
11
個人情報データベース
11A
ユーザＩＤ　氏名　生年月日　住所　性別　ハンドル名
honjo　本城信輔　1969.9.17　神奈川県…　男　JBoy
nanako　松島○○子　1969.1.12　東京都…　女　なでしこ
70
閲体者
①サーバ上の掲示板に、
Jboyによる不適正な
書き込みがあることを伝える
30
サーバ
②該当する書き込みを特定し、
対応するチケットＩＤを特定する
③Jboyが不適正な書き込みを
したことを伝える。
チケットＩＤを送信する。
④個人情報データベースを検索し、
Jboyは、ユーザhonjoであることが
分かる
⑤警告
20
ユーザ
honjo

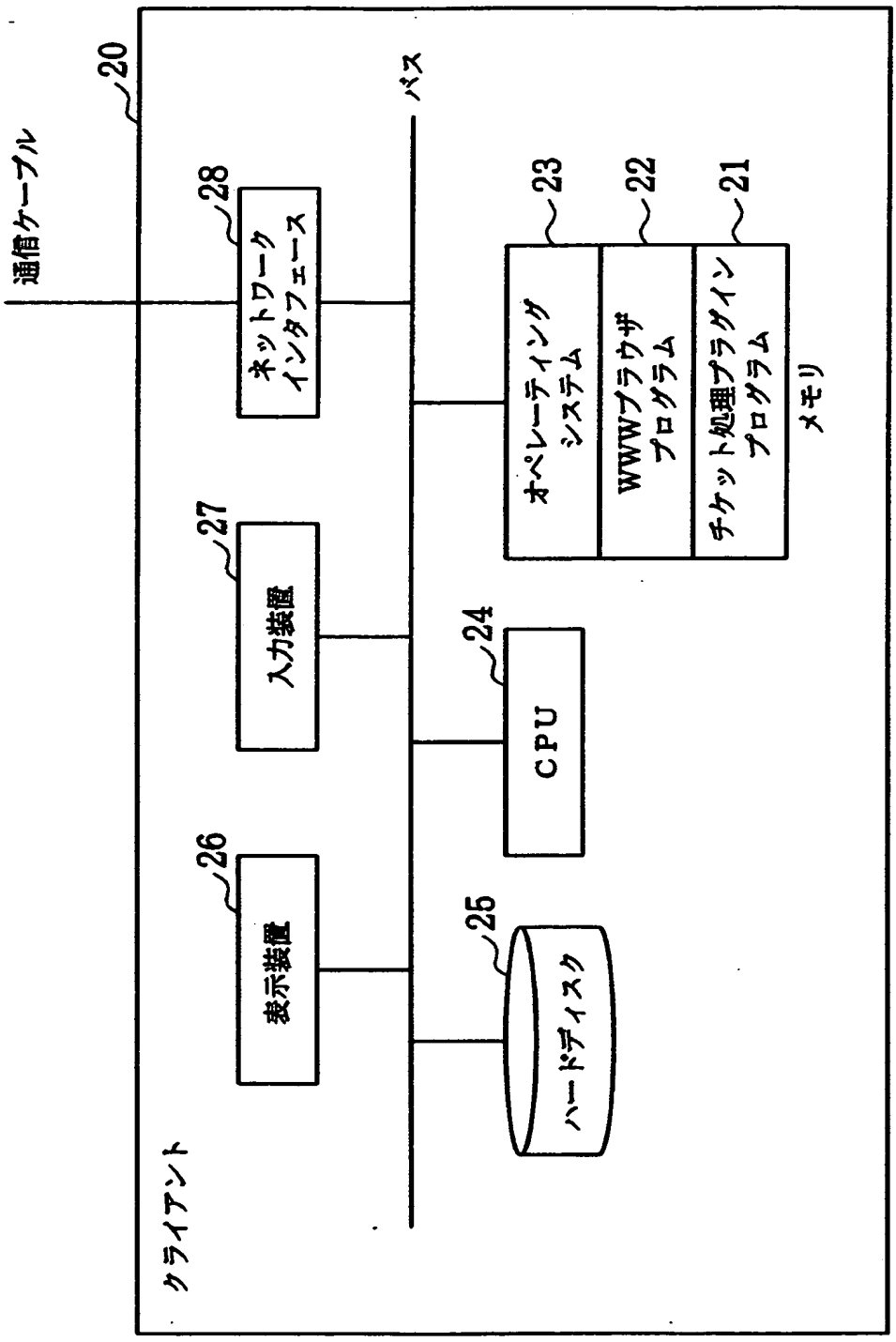
【図３】


課題の解決手段２（性別によるアクセス管理）
10
信頼できる第３者機関ＡＢＣ
11
個人情報データベース
11A
ユーザＩＤ　氏名　生年月日　住所　性別　ハンドル名
honjo　本城信輔　1969.9.17　神奈川県…　男　JBoy
nanako　松島ＯＯ子　1969.1.12　東京都…　女　なでしこ
30
サーバ
サーバ・ポリシ
掲示板Ａ：認証されたハンドル名
化粧品ページＢ：女性
成人向けページＣ：１８歳以上
⑥チケットを検証し、女性であるので
アクセスを許可する。
①化粧品ページＢに書き込み希望
②要チケット
31
サーバ・ポリシ
⑤化粧品ページＢに書き込み希望
12
チケット
⑦化粧品ページ
③チケット発行希望
性別の証明
20
ユーザ
nanako
④チケット送信
12
チケット
ＩＤ：98765432１@ＡＢＣ
このユーザは、女性です。
ＡＢＣによるデジタル署名

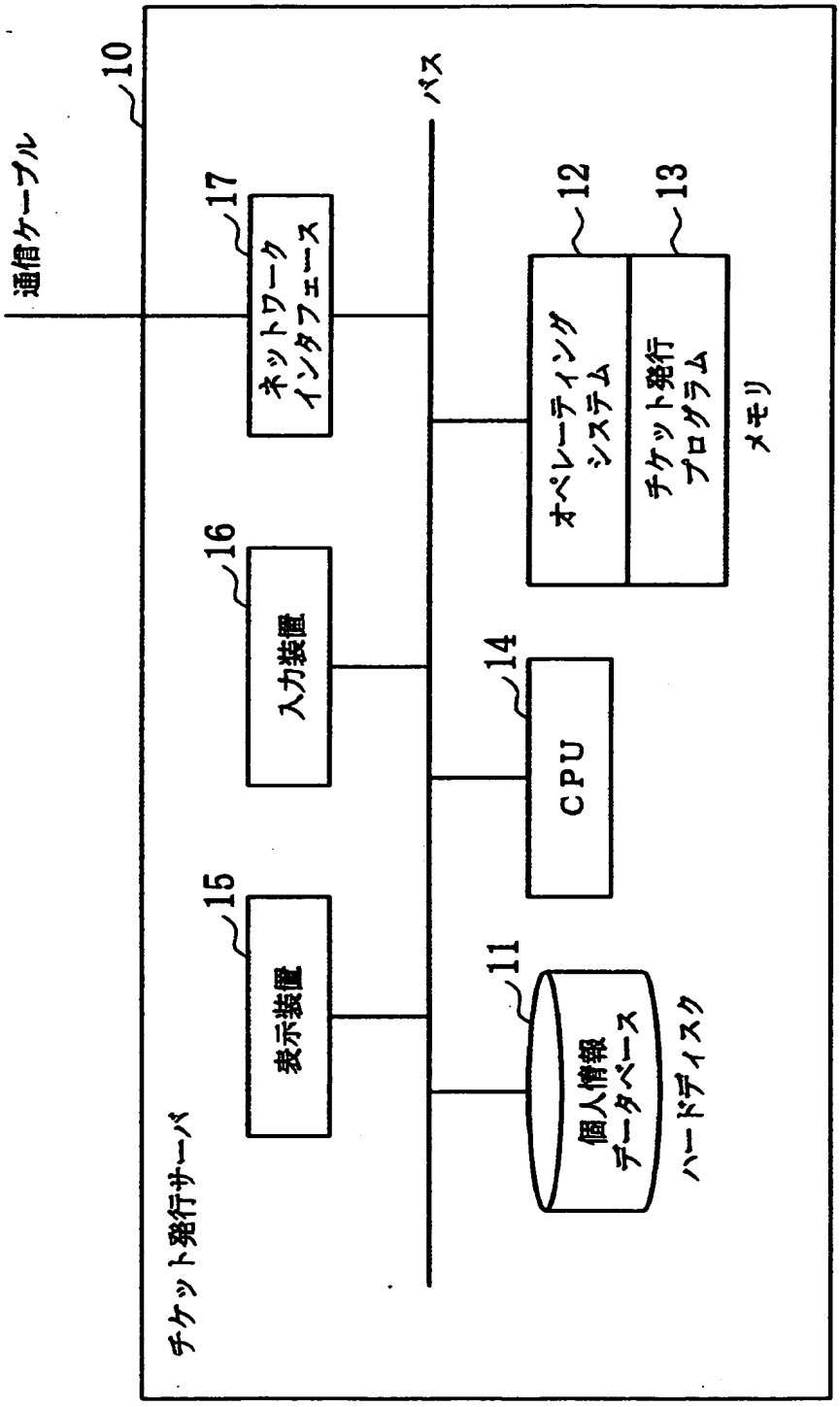
【図４】


実施例１：ネットワークの構成
40
ネットワーク
10
チケット発行サーバ
個人情報データベース
50
インターネット
32
30
チケット認証・アクセス管理部
WWWサーバ
20
21
チケット処理
プラグイン
プログラム
22
WWWブラウザ　クライアント
31
サーバ
・
ポリシ

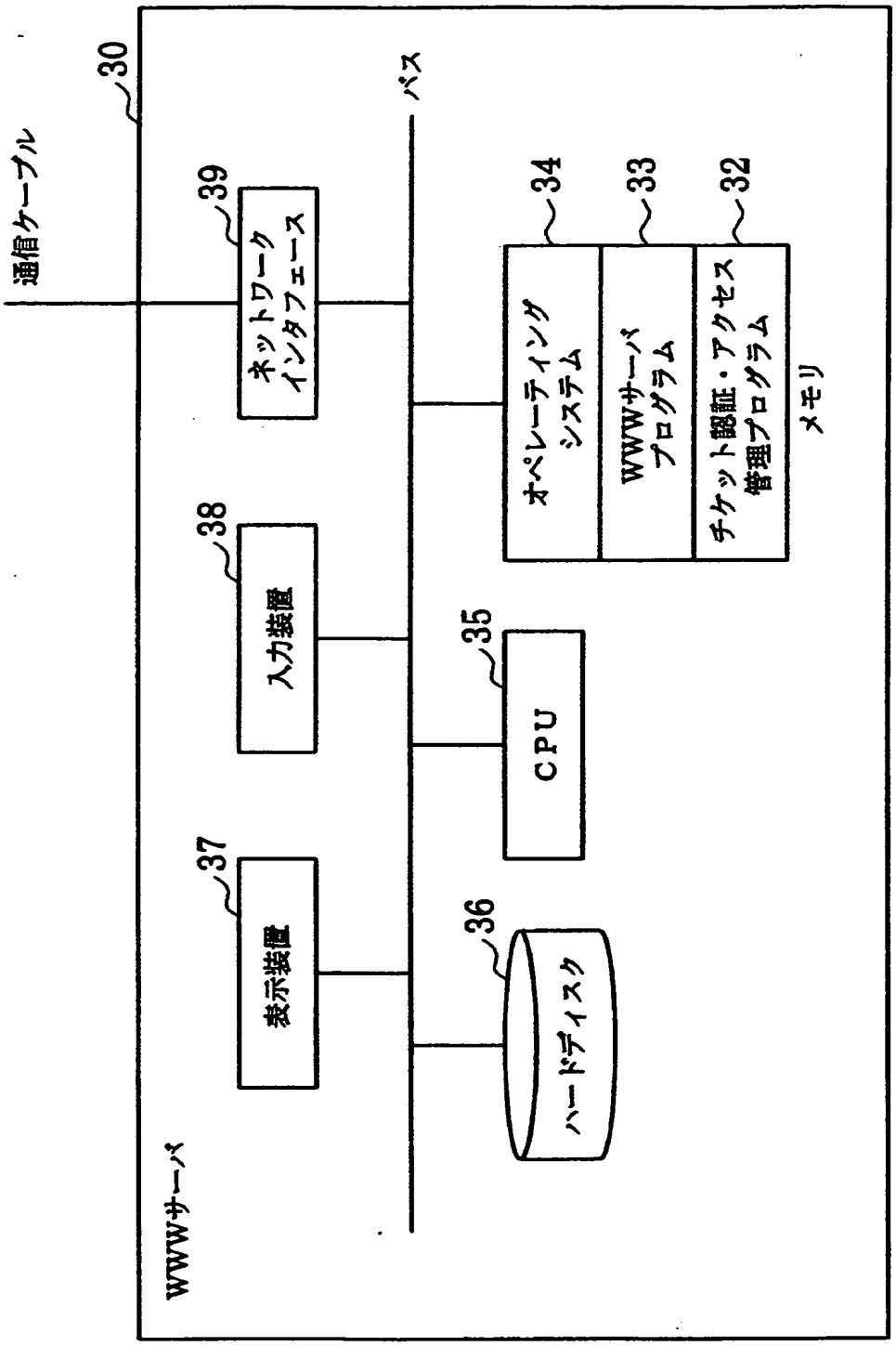
【図５】


20
通信ケーブル
28
ネットワーク
インタフェース
バス
23
22
21
オペレーティング
システム
WWWブラウザ
プログラム
チケット処理プラグイン
プログラム
メモリ
27
入力装置
24
CPU
26
表示装置
25
ハードディスク
クライアント

【図６】


チケット発行サーバ
10
通信ケーブル
17
ネットワーク
インタフェース
バス
12
オペレーティング
システム
13
チケット発行
プログラム
メモリ
16
入力装置
14
CPU
15
表示装置
11
個人情報
データベース
ハードディスク

【図７】


WWWサーバ
30
通信ケーブル
バス
39
ネットワーク
インタフェース
38
入力装置
37
表示装置
36
ハードディスク
35
CPU
34
オペレーティング
システム
33
WWWサーバ
プログラム
32
チケット認証・アクセス
管理プログラム
メモリ

## 実施例１：個人情報データベース

| ユーザＩＤ | 氏名 | 連絡先 | 生年月日 | 性別 | ハンドル名 | 所属 | メールアドレス |
|---|---|---|---|---|---|---|---|
| yamada | 山田花子<br>Hanako<br>Yamada | 大阪府…<br>1-21-31 | 1975.1.1 | 女 | 花子 | 総務部 | abc@def.co.jp |
| ichiro | 鈴木一郎<br>Ichiro Suzuki | 愛知県…<br>1-2-3 | 1960.12.1 | 男 | イチロー | 技術部 | pqr@xyz.co.jp |
| | | | | | | | |



特２０００－３２０６４５

出証特２００１－３０５３００６

## 実施例１：サーバ・ポリシ

サーバ：ｗｗｗ．ａｂｃ．ｃｏｍ

ディレクトリ：/ｃｇｉ－ｂｉｎ/ｂｂｓ/
　サービス：掲示板
　　必要な情報：ハンドル名、要承認、開示
　　必要な情報：氏名、要承認、非開示
　　必要な情報：連絡先、要承認、非開示

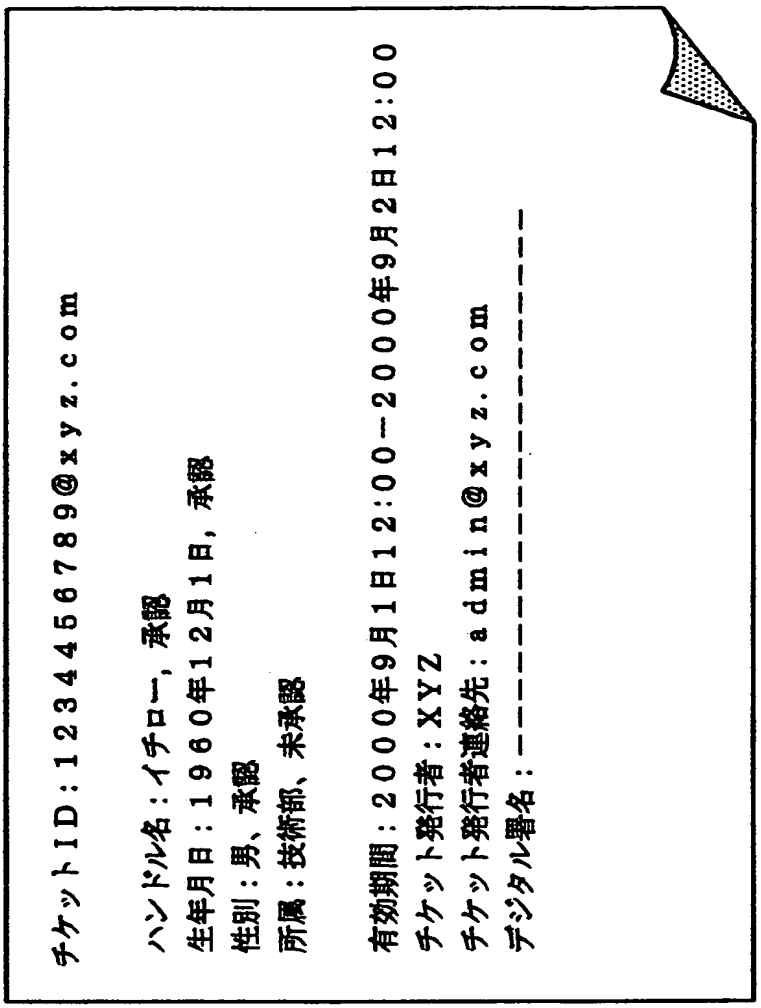
ディレクトリ：/ｗｏｍｅｎ/
　サービス：女性専用ページ
　　必要な情報：ハンドル名、要承認、開示
　　必要な情報：性別＝“女”，要承認、開示

ディレクトリ：/ｖｉｏｌｅｎｃｅ/
　サービス：映画情報ページ（暴力シーン・性的なシーンあり）
　　必要な情報：年齢>＝“１８”，要承認、開示

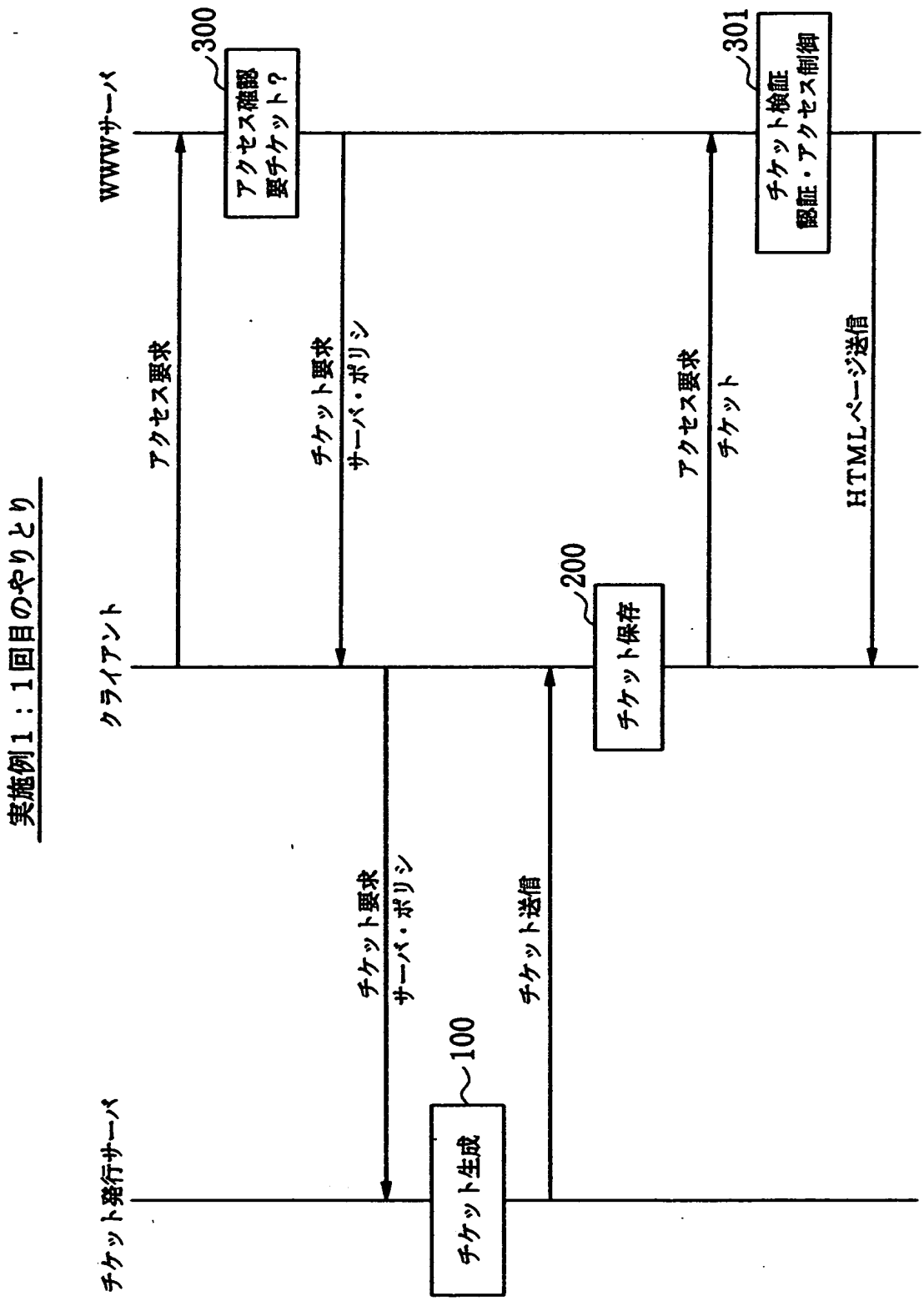
有効期間：２０００年5月1日１２：００－２０００年１０月２日１２：００

【図１０】

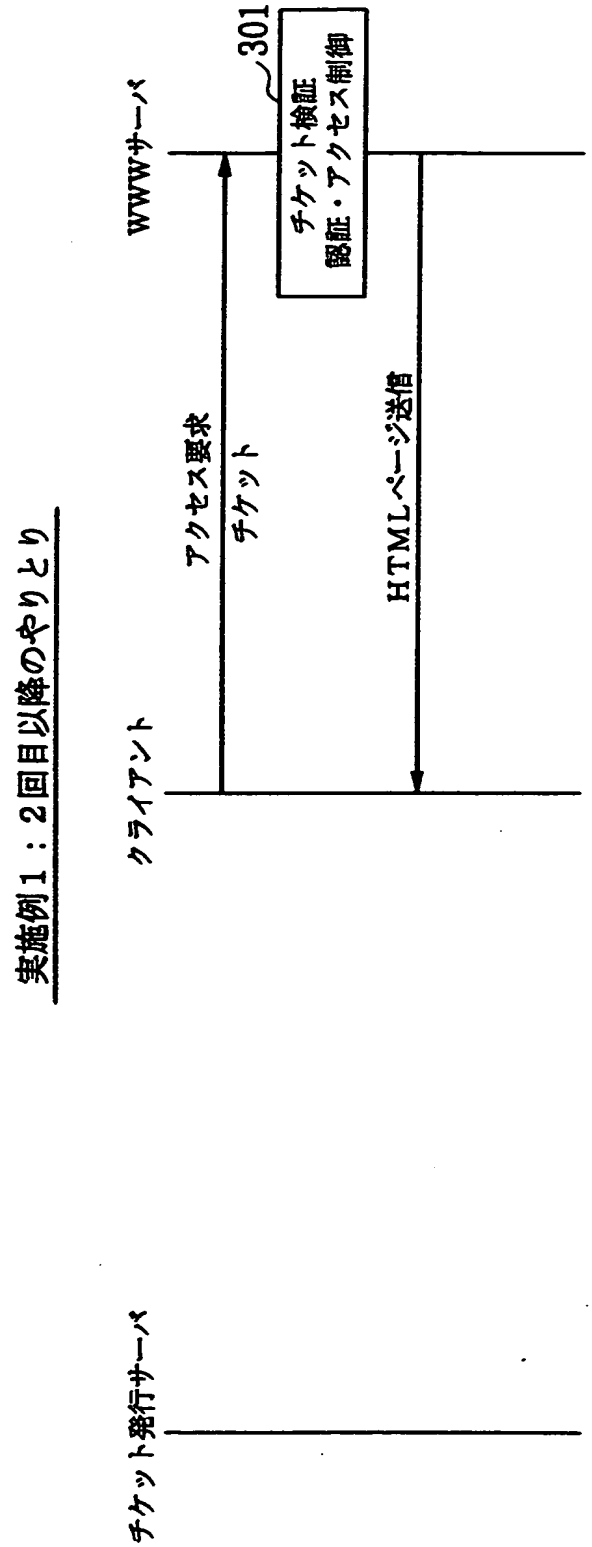
実施例１：チケット



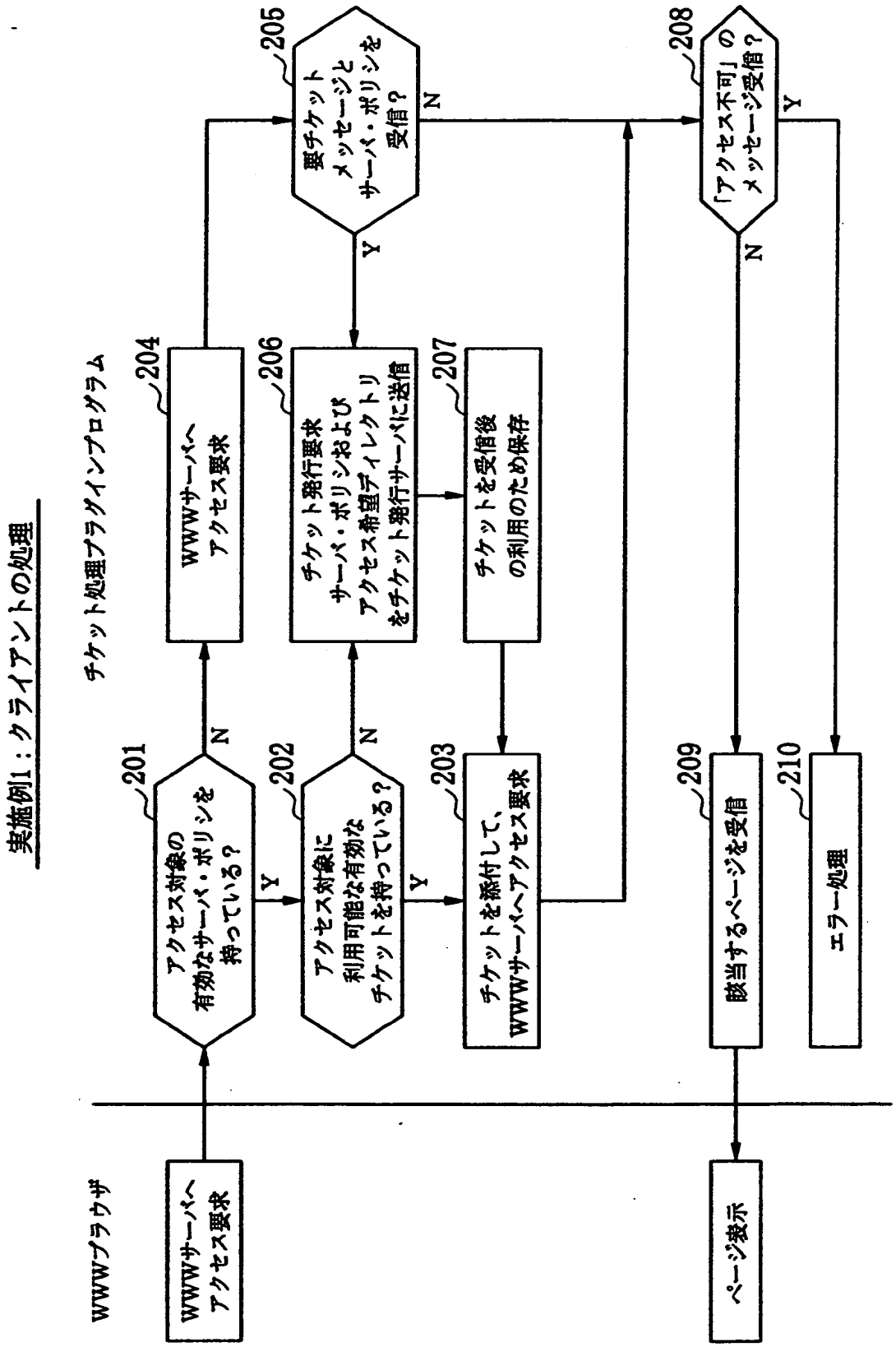
【図１１】


実施例１：１回目のやりとり
WWWサーバ
クライアント
チケット発行サーバ
300
アクセス確認
要チケット？
301
チケット検証
認証・アクセス制御
200
チケット保存
100
チケット生成
アクセス要求
チケット要求
サーバ・ポリシ
チケット要求
サーバ・ポリシ
チケット送信
アクセス要求
チケット
HTMLページ送信

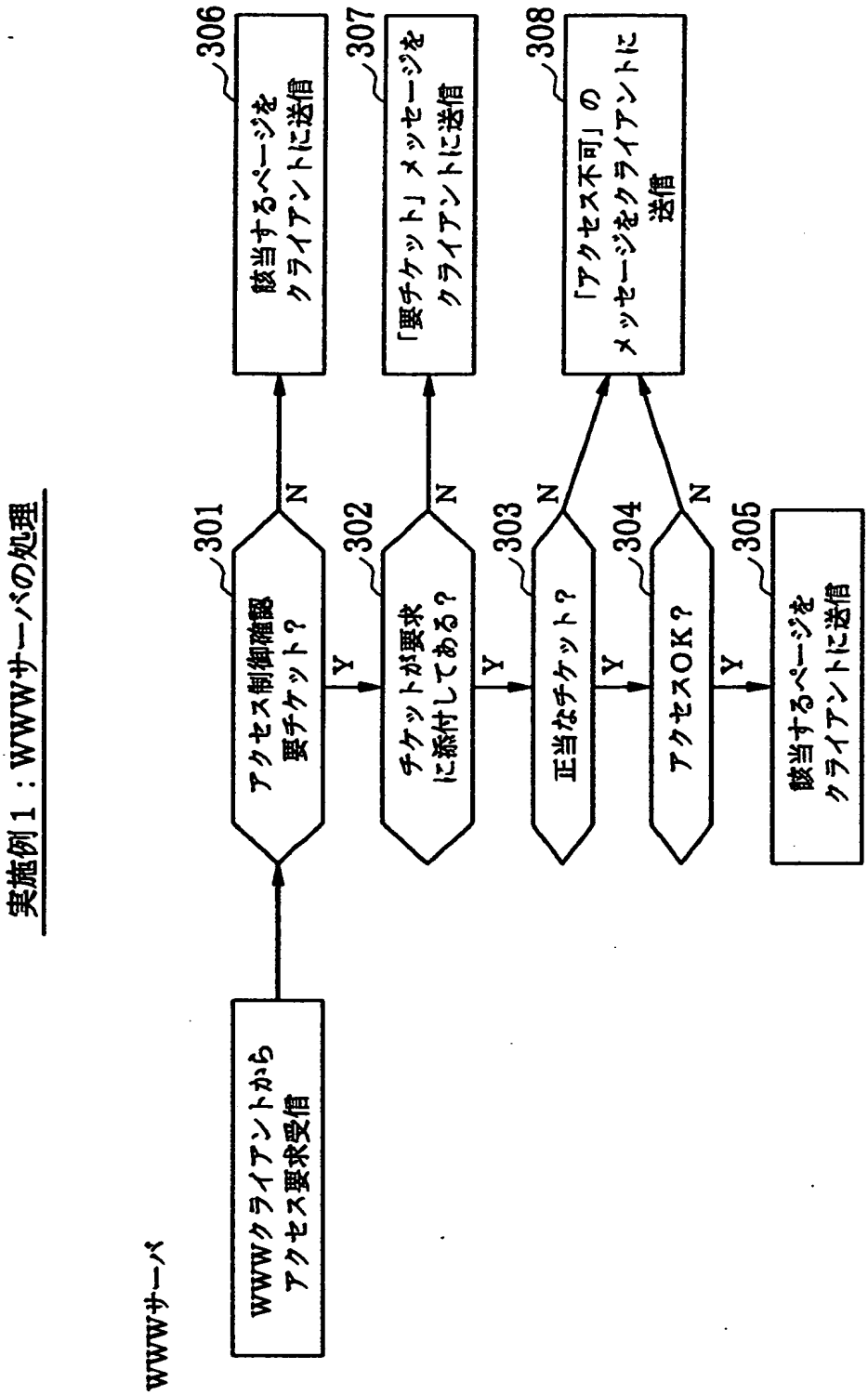
【図１２】


実施例１：２回目以降のやりとり
クライアント
WWWサーバ
チケット発行サーバ
301
チケット検証
認証・アクセス制御
アクセス要求
チケット
HTMLページ送信

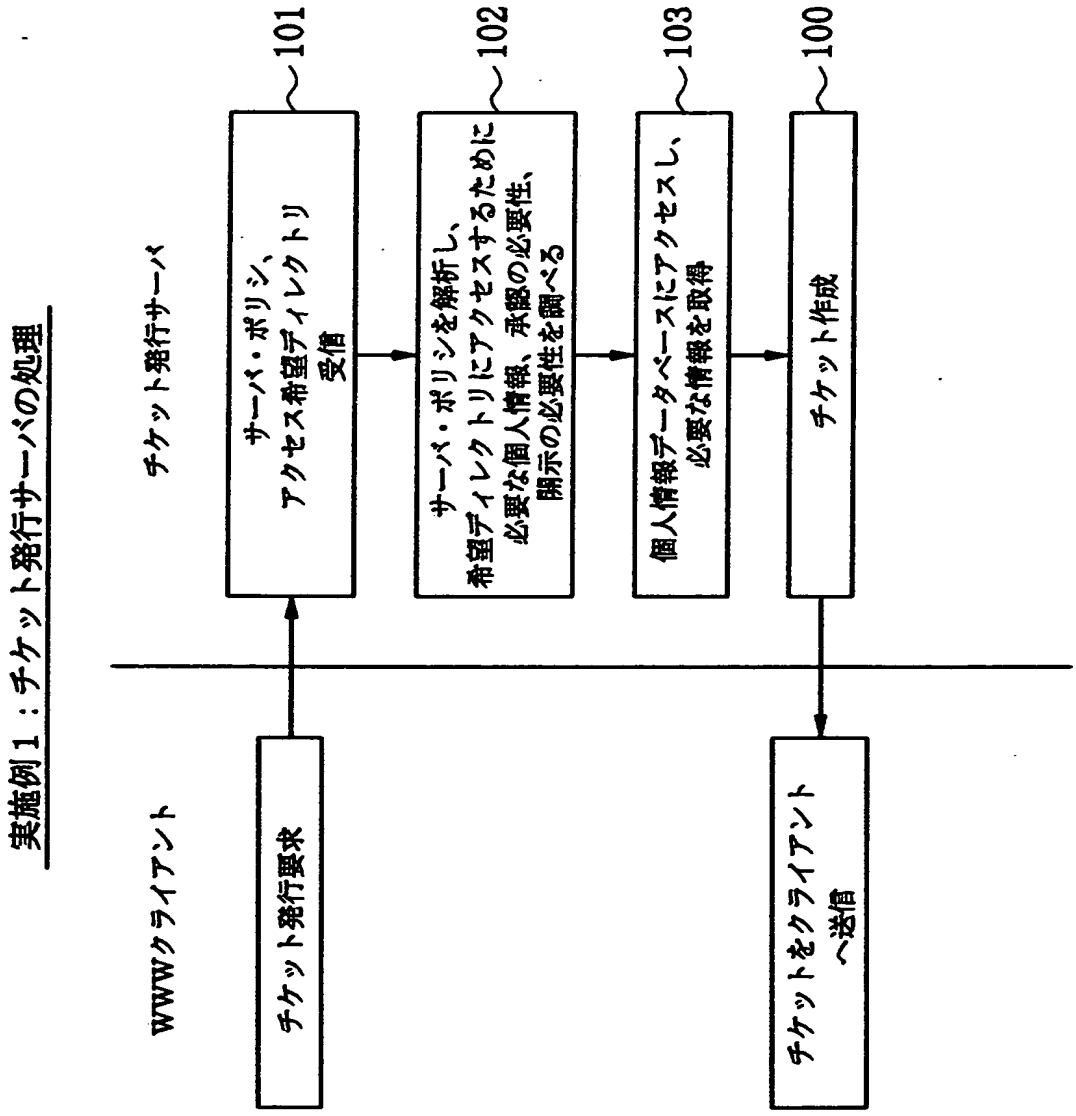
【図１３】


実施例1：クライアントの処理
チケット処理プラグインプログラム
WWWブラウザ
WWWサーバへ
アクセス要求
201
アクセス対象の
有効なサーバ・ポリシを
持っている？
202
アクセス対象に
利用可能な有効な
チケットを持っている？
203
チケットを添付して、
WWWサーバへアクセス要求
204
WWWサーバへ
アクセス要求
205
要チケット
メッセージと
サーバ・ポリシを
受信？
206
チケット発行要求
サーバ・ポリシおよび
アクセス希望ディレクトリ
をチケット発行サーバに送信
207
チケットを受信後
の利用のため保存
208
「アクセス不可」の
メッセージ受信？
209
該当するページを受信
210
エラー処理
ページ表示
N
Y
N
Y
N
Y

【図１４】


実施例１：WWWサーバの処理
WWWサーバ
WWWクライアントから
アクセス要求受信
301
アクセス制御確認
要チケット？
N
Y
306
該当するページを
クライアントに送信
302
チケットが要求
に添付してある？
N
Y
307
「要チケット」メッセージを
クライアントに送信
303
正当なチケット？
N
Y
308
「アクセス不可」の
メッセージをクライアントに
送信
304
アクセスOK？
N
Y
305
該当するページを
クライアントに送信

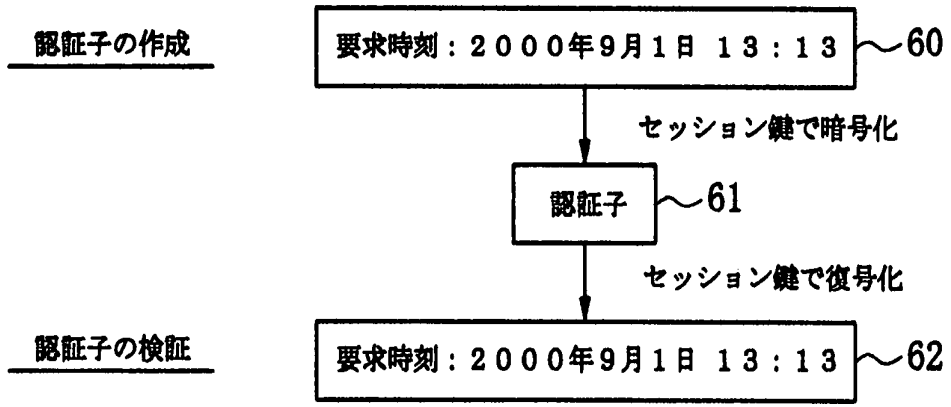
【図１５】


実施例１：チケット発行サーバの処理
WWWクライアント
チケット発行サーバ
チケット発行要求
101
サーバ・ポリシ、
アクセス希望ディレクトリ
受信
102
サーバ・ポリシを解析し、
希望ディレクトリにアクセスするために
必要な個人情報、承認の必要性、
開示の必要性を調べる
103
個人情報データベースにアクセスし、
必要な情報を取得
100
チケット作成
チケットをクライアント
へ送信

【図１６】


実施例２：チケット
チケットＩＤ：１２３４４５６７８９@ｘｙｚ.ｃｏｍ
ハンドル名：イチロー，承認
生年月日：１９６０年１２月１日，承認
性別：男、承認
所属：技術部、未承認
有効期間：２０００年９月１日１２:００－２０００年９月２日１２:００
チケット発行者：ＸＹＺ
チケット発行者連絡先：ａｄｍｉｎ@ｘｙｚ.ｃｏｍ
デジタル署名：－－－－－－－－－－－－－－－－－－－－－－－－
セッション鍵：ｘｘｘｘｘｘｘｘｘｘｘｘｘｘｘｘ
利用するWWWサーバの公開鍵で暗号化
暗号化されたチケット
WWWサーバとクライアントで共有するセッション鍵
(チケット発行サーバが生成)

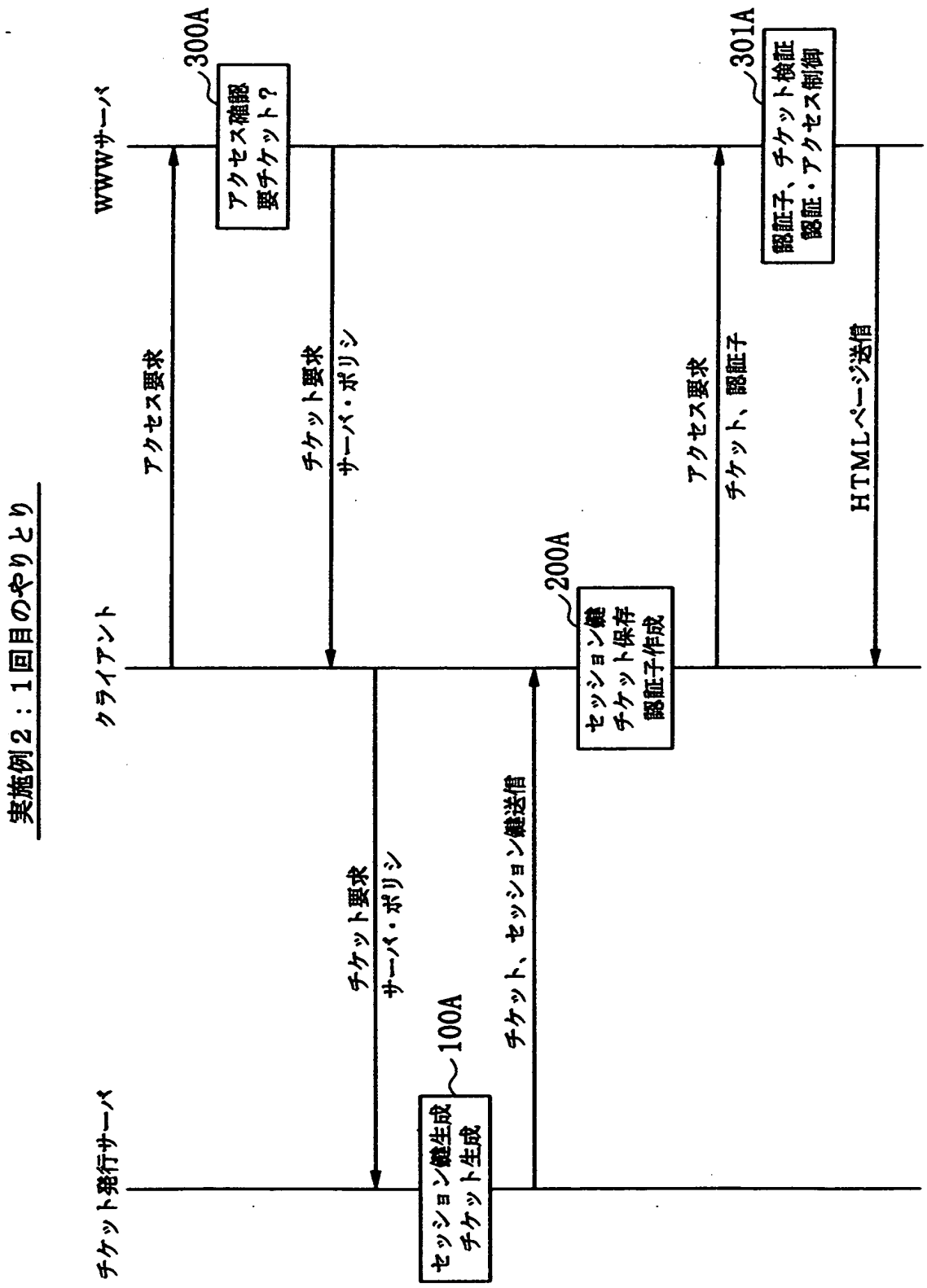
## 実施例２：認証子（チケットの正当な保持者であることを証明するためのもの）



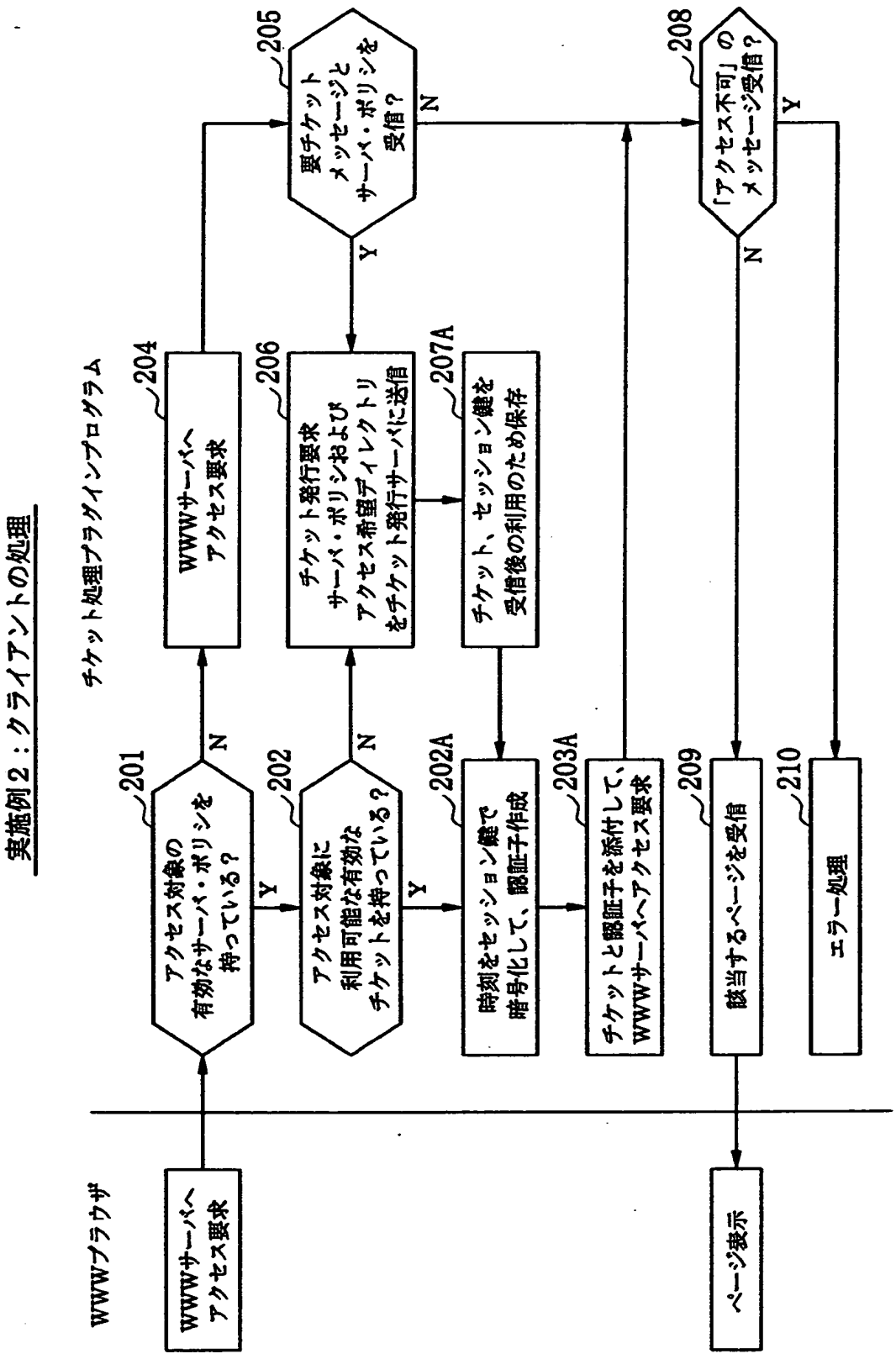

要求時刻が現在の時刻から許容範囲内にあるかどうか確認
（不正に他人が同じ認証子を再送するのを防ぐ）

注意）認証子を作ったり検証できる人＝セッション鍵を知っている人
つまり、クライアント（チケット発行サーバにセッション鍵を教えてもらう）
とWWWサーバ（チケットを復号化して、セッション鍵を取り出せる）
それ以外の人は、認証子を作ったり、検証したりすることはできない

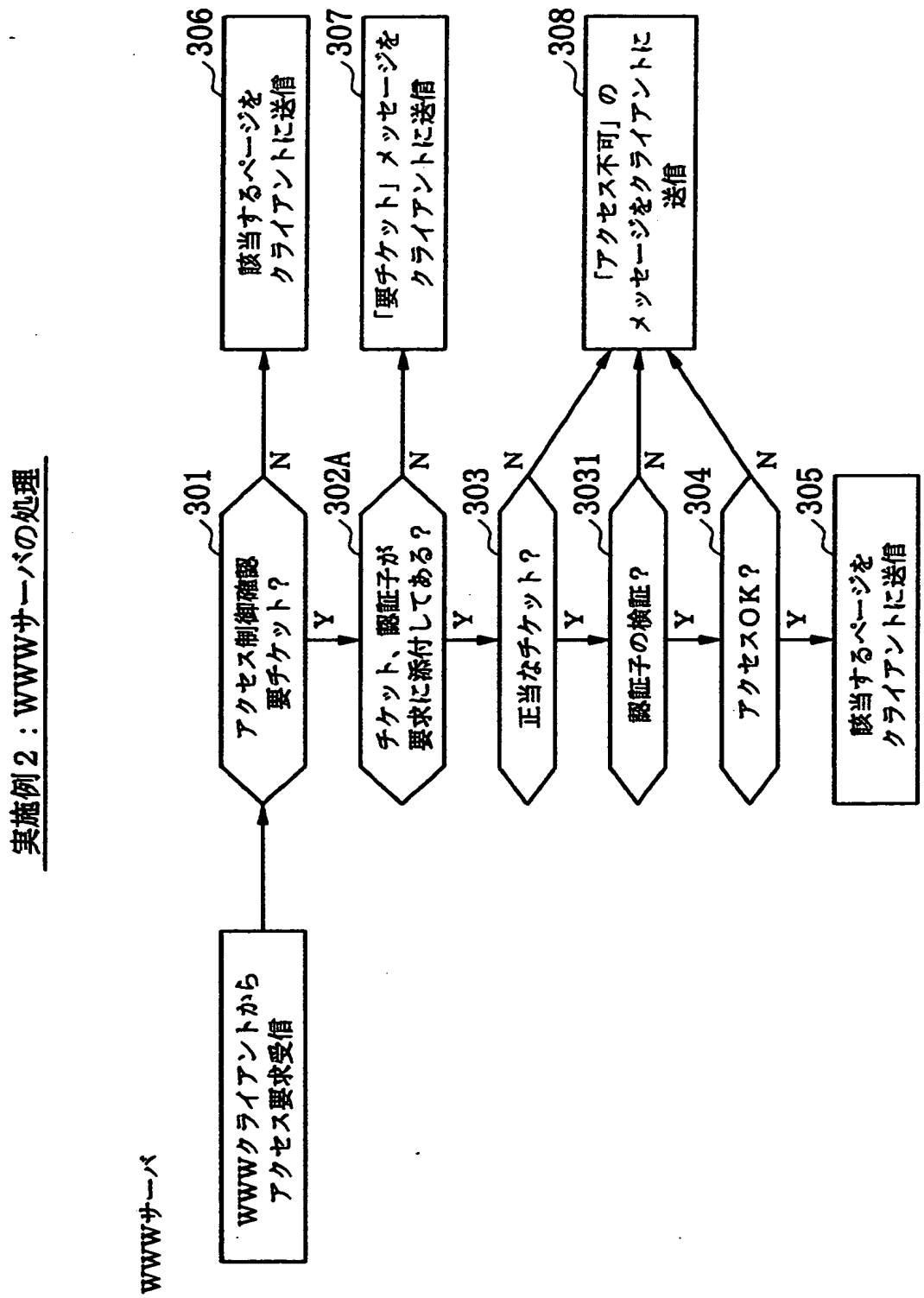
【図１８】


実施例２：１回目のやりとり
WWWサーバ
クライアント
チケット発行サーバ
300A
アクセス確認
要チケット？
301A
認証子、チケット検証
認証・アクセス制御
200A
セッション鍵
チケット保存
認証子作成
100A
セッション鍵生成
チケット生成
アクセス要求
チケット要求
サーバ・ポリシ
チケット、セッション鍵送信
アクセス要求
チケット、認証子
HTMLページ送信
チケット要求
サーバ・ポリシ

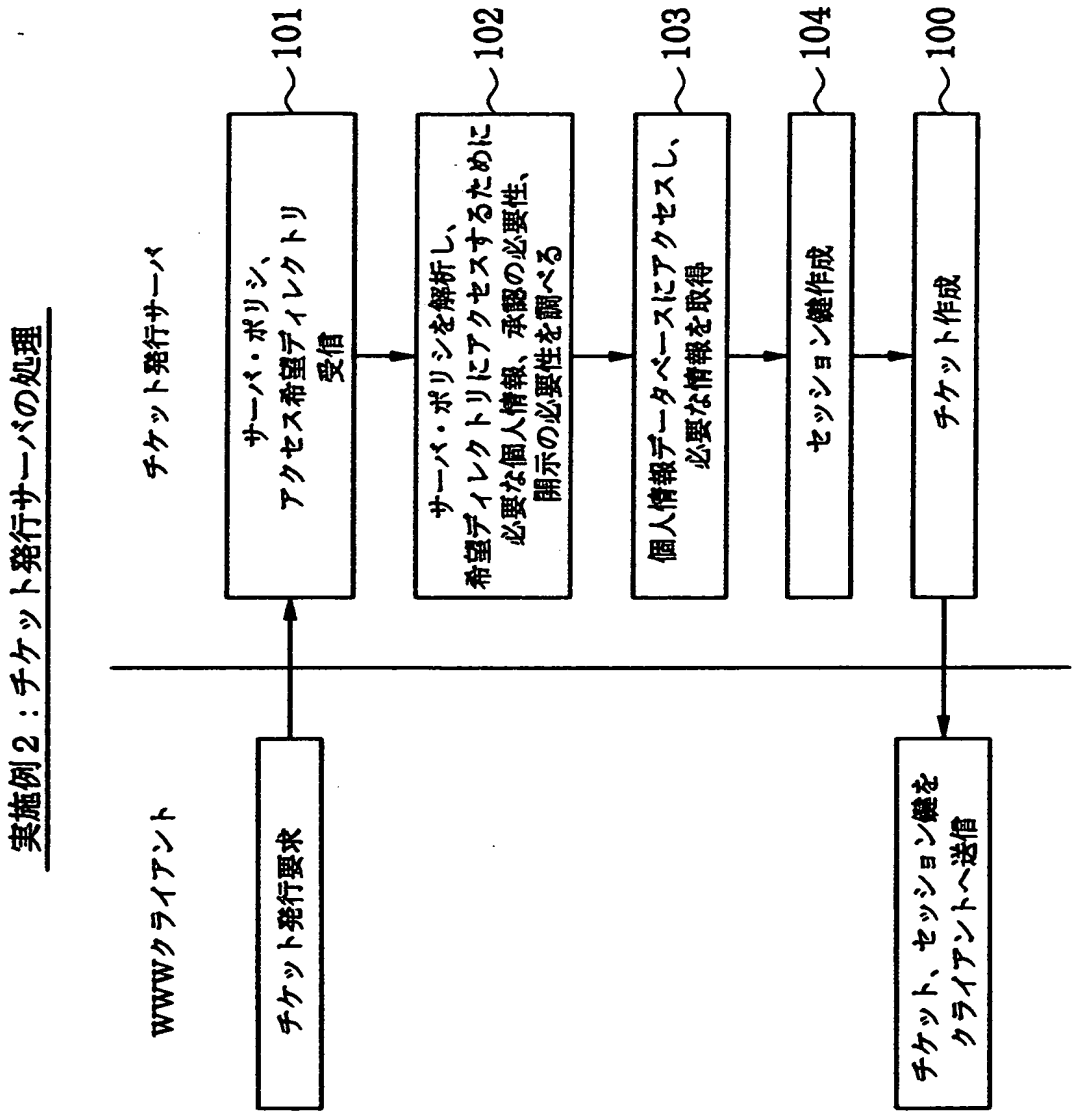
【図１９】


実施例２：クライアントの処理
WWWブラウザ
チケット処理プラグインプログラム
WWWサーバへアクセス要求
201
アクセス対象の有効なサーバ・ポリシを持っている？
N
Y
204
WWWサーバへアクセス要求
202
アクセス対象に利用可能な有効なチケットを持っている？
N
Y
206
チケット発行要求サーバ・ポリシおよびアクセス希望ディレクトリをチケット発行サーバに送信
205
要チケットメッセージとサーバ・ポリシを受信？
N
Y
207A
チケット、セッション鍵を受信後の利用のため保存
202A
時刻をセッション鍵で暗号化して、認証子作成
203A
チケットと認証子を添付して、WWWサーバへアクセス要求
208
「アクセス不可」のメッセージ受信？
Y
N
209
該当するページを受信
ページ表示
210
エラー処理

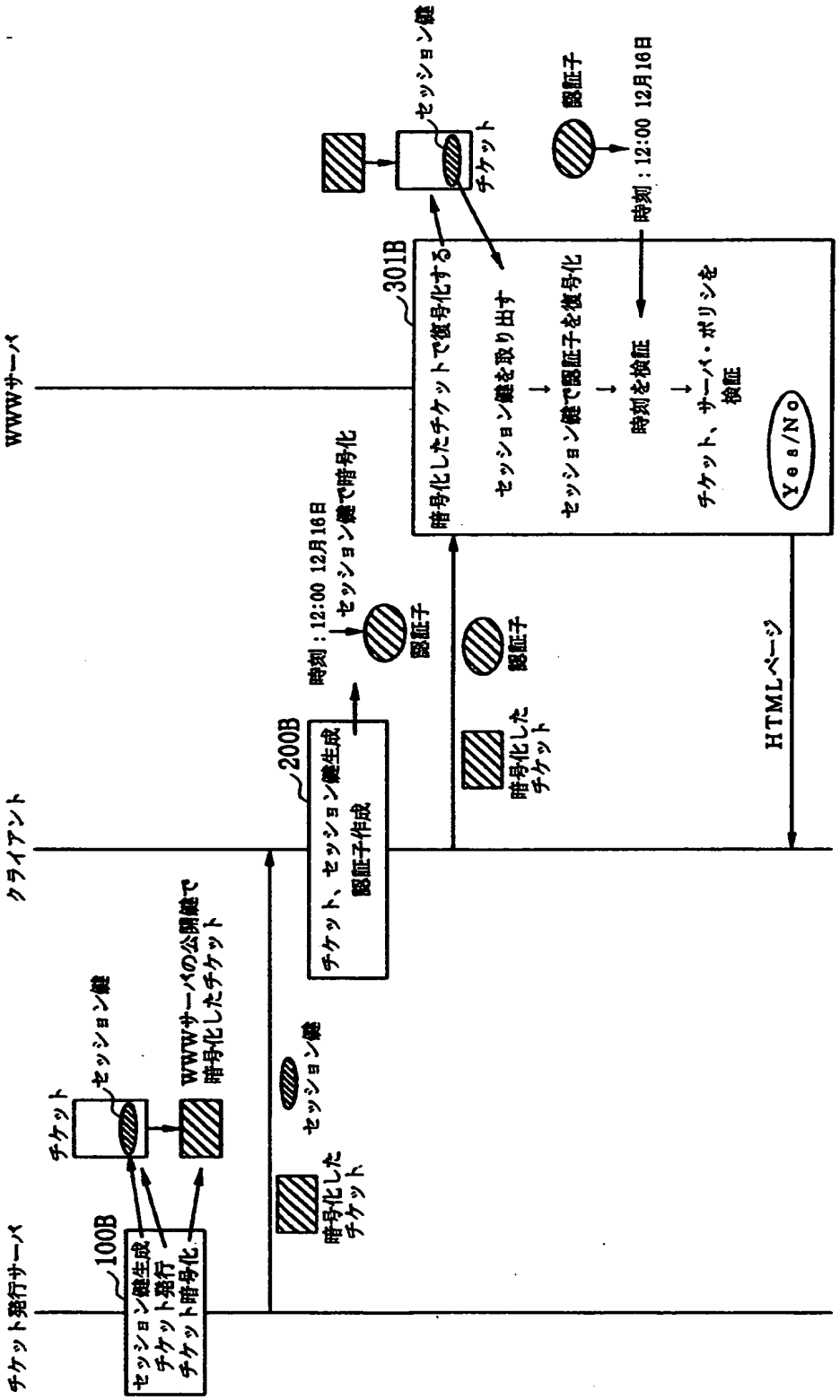
【図２０】


実施例２：WWWサーバの処理
WWWサーバ
WWWクライアントから
アクセス要求受信
301
アクセス制御確認
要チケット？
N
Y
306
該当するページを
クライアントに送信
302A
チケット、認証子が
要求に添付してある？
N
Y
307
「要チケット」メッセージを
クライアントに送信
303
正当なチケット？
N
Y
308
「アクセス不可」の
メッセージをクライアントに
送信
3031
認証子の検証？
N
Y
304
アクセスOK？
N
Y
305
該当するページを
クライアントに送信

【図２１】


実施例２：チケット発行サーバの処理
WWWクライアント
チケット発行サーバ
チケット発行要求
101
サーバ・ポリシ、
アクセス希望ディレクトリ
受信
102
サーバ・ポリシを解析し、
希望ディレクトリにアクセスするために
必要な個人情報、承認の必要性、
開示の必要性を調べる
103
個人情報データベースにアクセスし、
必要な情報を取得
104
セッション鍵作成
100
チケット作成
チケット、セッション鍵を
クライアントへ送信

【図２２】


チケット発行サーバ
100B
セッション鍵生成
チケット発行
チケット暗号化
チケット
セッション鍵
WWWサーバの公開鍵で
暗号化したチケット
クライアント
セッション鍵
暗号化した
チケット
200B
チケット、セッション鍵生成
認証子作成
時刻：12:00 12月16日
セッション鍵で暗号化
認証子
暗号化した
チケット
認証子
HTMLページ
WWWサーバ
301B
暗号化したチケットで復号化する
セッション鍵を取り出す
セッション鍵で認証子を復号化
時刻を検証
チケット、サーバ・ポリシを
検証
Yes/No
時刻：12:00 12月16日
認証子
セッション鍵
チケット

【書類名】　　要約書

【要約】

【課題】信頼のある個人情報を基にアクセス管理を可能にするとともに、個人情報を秘匿しながらの身元保証を可能にする。

【解決手段】①ユーザ２０は個人情報を第三者機関１０に登録する。②③アクセス制御を行うサーバ３０は、その条件を記載したサーバ・ポリシ３１を設定する。サーバ・ポリシの記載内容としては、対象ディレクトリ、必要な情報、情報の開示レベル、情報の承認が必要か否かである。④ユーザ２０は、第三者機関１０に必要な情報を承認してもらうために、⑤チケット１２を発行してもらう。⑥ユーザ２０は、チケット１２をサーバ３０に提示、サーバ３０は、チケット１２の内容とサーバ・ポリシ３１とを照らし合わせ、アクセス可能か否かを判断する。⑦ＯＫの場合には、掲示板に書き込みＯＫをユーザ２０に返送する。

【選択図】　　図１

# 認定・付加情報

| | |
|---|---|
| 特許出願の番号 | 特願２０００－３２０６４５ |
| 受付番号 | ５００００１３５７８５８ |
| 書類名 | 特許願 |
| 担当官 | 佐藤　一博　　１９０９ |
| 作成日 | 平成１２年１１月　２日 |

＜認定情報・付加情報＞

【提出日】　平成12年10月20日

【特許出願人】

【識別番号】　000005108

【住所又は居所】　東京都千代田区神田駿河台四丁目６番地

【氏名又は名称】　株式会社日立製作所

【代理人】

【識別番号】　100077274

【住所又は居所】　東京都新宿区西新宿１丁目２３番１号　新宿千葉ビル

【氏名又は名称】　磯村　雅俊

【復代理人】　申請人

【識別番号】　100102587

【住所又は居所】　東京都新宿区西新宿１丁目２３番１号　新宿千葉ビル

【氏名又は名称】　渡邉　昌幸

次頁無

# 出　願　人　履　歴　情　報

識別番号　　〔０００００５１０８〕

１．変更年月日　　１９９０年　８月３１日
［変更理由］　新規登録
住　所　東京都千代田区神田駿河台４丁目６番地
氏　名　株式会社日立製作所